CISSP Study Booklet on Cryptography

This simple study booklet is based directly on the ISC^2 CBKdocument.

This guide does not replace in any way the outstanding value of the CISSP Seminar and the fact that you must have been involved into the security field for at least a few years if you intend to take the CISSP exam. This booklet simply intend to make your life easier and to provide you with a centralized resource for this particular domain of expertise.

This guide was created by Clement Dupuis on 5th April 1999

WARNING:

As with any security related topic, this is a living document that will and must evolve as other people read it and technology evolves. Please feel free to send me comments or input to be added to this document. Any comments, typo correction, etc... are most welcome and can be send directly to:
cdupuis@uniconseil.com

DISTRIBUTION AGREEMENT:

Cryptography

Description :

The Cryptography domain addresses the principles, means, and methods of securing information to ensure its integrity, confidentiality, and authenticity.

Expected Knowledge :

The professional should fully understand :

- Basic concepts within cryptography.
- Public and private key algorithms in terms of their applications and uses.
- Cryptography algorithm construction, key distribution, key management, and methods of attack
- Applications, constructions, and use of digital signatures
- Principles of authenticity of electronic transactions and non-repudiation

The CISSP can meet the expectations defined above by understanding such Operations Security key areas of knowledge as :

- Authentication
- Certificate authority
- Digital Signatures/Non-Repudiation
- Encryption
- Error Detecting/Correcting features
- Hash Functions
- Kerberos
- Key Escrow
- Messages Digest

- MD5
- SHA
- HMAC
- One-Time cipher keys
- Private Key Algorithms
- Applications and Uses
- Algorithm Methodology
- Key Distribution and Management
- Key Generation/Distribution
- Key Recovery
- Key Storage and Destruction
- Key Strenth
    - Complexity
    - Secrecy
    - Weak keys
- Method of attack
- Public key Algorithms
- Application and uses
- Algorithm Methodology
- Key Distribution and Management
- Key Distribution and Management
- Key Storage and Destruction
- Key Recovery
- Key Strength
- Complexity
- Secrecy
- Weak Keys

- Methos of attack
- Stream Cipher

Examples of Knowledgeability

Describe the ancient history of Cryptography

CISSP Seminar :

- First appearance – Egypt > 4000 years ago
- Scytale –Sparta – 400 BC
- Paper wrapped on rod
- Text written on paper
- Paper removed – cipher text
- Ceasar Cipher – Julius Caesar – Rome – 49 BC
- 7th Century AD – Arabs
- Cipher Alphabets in magic – 855 AD
- Leon Batista Alberti's cipher disk – Italy – 1459 AD
- Thomas Jefferson ciphering device- 1790- Stack of 26 disks
- Each disk contained alphabet around face of edge in different order
- Positioning bar attached to align letters in row
- Created message by moving each disk to proper letter
- Bar rotated fixed amount (the key)
- Letters around new position (cipher text)
- ROT 13 – Many UNIX system
- Shifts letters 13 places
- Not secured from frequency analysis
- Encrypted twice-plain text

From Cryptography FAQ :

The story begins: When Julius Caesar sent messages to his trusted acquaintances, he didn't trust the messengers. So he replaced every A by a D, every B by a E, and so on through the alphabet. Only someone who knew the ``shift by 3'' rule could decipher his messages.

From CME's Cryptography Timeline : (if you are really interested in knowing it all, or else jump over)

Date	C or G	Source	Info
about 1900 BC	civ	Kahn p.71	An Egyptian scribe used non-standard hieroglyphs in an inscription. Kahn lists this as the first documented example of written cryptography.
1500 BC	Civ	Kahn p.75	A Mesopotamian tablet contains an enciphered formula for the making of glazes for pottery.
500-600 BC	Civ	Kahn p.77	Hebrew scribes writing down the book of Jeremiah used a reversed-alphabet simple substitution cipher known as ATBASH. (Jeremiah started dictating to Baruch in 605 BC but the chapters containing these bits of cipher are attributed to a source labeled ``C'' (believed not to be Baruch) which could be an editor writing after the Babylonian exile in 587 BC, someone contemporaneous with Baruch or even Jeremiah himself.) ATBASH was one of a few Hebrew ciphers of the time.
487 BC	Govt	Kahn p.82	The Greeks used a device called the ``skytale'' -- a staff around which a long, thin strip of leather was wrapped and written on. The leather was taken off and worn as a belt. Presumably, the recipient would have a matching staff and the encrypting staff would be left home. **[Note: an article in Cryptologia late in 1998 makes the case that the cryptographic use of the skytale may be a myth.]**
50-60 BC	Govt	Kahn p.83	**Julius Caesar** (100-44 BC) used a simple substitution with the normal alphabet (just shifting the letters a fixed amount) in government communciations. This cipher was less strong than ATBASH, by a small amount, but in a day when few people read in the first place, it was good enough. He also used tansliteration of Latin into Greek letters and a number of other simple ciphers.
0-400?	Civ	Burton	The Kama Sutra of Vatsayana lists cryptography as the 44th and 45th of 64 arts (yogas) men and women should know and practice. The date of this work is unclear but is believed to be between the first and fourth centuries, AD. [Another expert, John W. Spellman, will commit only to the range between the 4th century BC and the 5th century AD.] Vatsayana says that his Kama Sutra is a compilation of much earlier works, making the dating of the

			cryptography references even more uncertain. Part I, Chapter III lists the 64 arts and opens with: ``Man should study the Kama Sutra and the arts and sciences subordinate thereto [....] Even young maids should study this Kama Sutra, along with its arts and sciences, before marriage, and after it they should continue to do so with the consent of their husbands.'' These arts are clearly not the province of a government or even of academics, but rather are practices of laymen. In this list of arts, the 44th and 45th read: • The art of understanding writing in cipher, and the writing of words in a peculiar way. • The art of speaking by changing the forms of words. It is of various kinds. Some speak by changing the beginning and end of words, others by adding unnecessary letters between every syllable of a word, and so on.
200's	Civ	Kahn p.91	``The so-called Leiden papyrus [...] employs cipher to conceal the crucial portions of important [magic] recipes''.
725-790?	Govt/(civ)	Kahn p.97	**Abu `Abd al-Rahman al-Khalil ibn Ahmad ibn `Amr ibn Tammam al Farahidi al-Zadi al Yahmadi** wrote a (now lost) book on cryptography, inspired by his solution of a cryptogram in Greek for the Byzantine emperor. His solution was based on known (correctly guessed) plaintext at the message start -- a standard cryptanalytic method, used even in WW-II against Enigma messages.
855	Civ	Kahn p.93	**Abu Bakr Ahmad ben `Ali ben Wahshiyya an-Nabati** published several cipher alphabets which were traditionally used for magic.
---	Govt	Kahn p.94	``A few documents with ciphertext survive from the Ghaznavid government of conquered Persia, and one chronicler reports that high officials were supplied with a personal cipher before setting out for new posts. But the general lack of continuity of Islamic states and the consequent failure to develop a permanent civil service and to set up permanent embassies in other countries militated against cryptography's more widespread use.''
1226	Govt	Kahn p.106	``As early as 1226, a faint political cryptography appeared in the archives of Venice, where dots or crosses replaced the vowels in a few scattered words.''
about 1250	Civ	Kahn p.90	**Roger Bacon** not only described several ciphers but wrote: ``A man is crazy who writes a secret in any other way than one which will conceal it from

			the vulgar.''
1379	Govt/civ	Kahn p.107	**Gabrieli di Lavinde** at the request of Clement VII, compiled a combination substitution alphabet and small code -- the first example of the *nomenclator* Kahn has found. This class of code/cipher was to remain in general use among diplomats and some civilians for the next 450 years, in spite of the fact that there were stronger ciphers being invented in the meantime, possibly because of its relative convenience.
1300's	Govt	Kahn p.94	**`Abd al-Rahman Ibn Khaldun** wrote "The Muqaddimah", a substantial survey of history which cites the use of ``names of perfumes, fruits, birds, or flowers to indicate the letters, or [...] of forms different from the accepted forms of the letters'' as a cipher among tax and army bureaus. He also includes a reference to cryptanalysis, noting ``Well-known writings on the subject are in the possession of the people.'' *[p.97]*
1392	Civ	Price p.182-7	"The Equatorie of the Planetis", possibly written by **Geoffrey Chaucer**, contains passages in cipher. The cipher is a simple substitution with a cipher alphabet consisting of letters, digits and symbols.
1412	Civ	Kahn p.95-6	**Shihab al-Din abu `l-`Abbas Ahmad ben `Ali ben Ahmad `Abd Allah al-Qalqashandi** wrote "Subh al-a `sha", a 14-volume Arabic encyclopedia which included a section on cryptology. This information was attributed to **Taj ad-Din `Ali ibn ad-Duraihim ben Muhammad ath-Tha`alibi al-Mausili** who lived from 1312 to 1361 but whose writings on cryptology have been lost. The list of ciphers in this work included both substitution and transposition and, for the first time, a cipher with multiple substitutions for each plaintext letter. Also traced to Ibn al-Duraihim is an exposition on and worked example of cryptanalysis, including the use of tables of letter frequencies and sets of letters which can not occur together in one word.
1466-7	Civ	Kahn p.127	**Leon Battista Alberti** (a friend of **Leonardo Dato**, a potifical secretary who might have instructed Alberti in the state of the art in cryptology) invented and published the first polyalphabetic cipher, designing a cipher disk (known to us as the Captain Midnight Decoder Badge) to simplify the process. This class of cipher was apparently not broken until the 1800's. Alberti also wrote extensively on the state of the art in ciphers, besides his own invention. Alberti also used his disk for enciphered code. These systems were much stronger than the nomenclator in use by the diplomats of the day and for centuries to come.

1473-1490	Civ	Kahn p.91	``A manuscript [...] by **Arnaldus de Bruxella** uses five lines of cipher to conceal the crucial part of the operation of making a philosopher's stone.''
1518	Civ	Kahn p.130-6	**Johannes Trithemius** wrote the first printed book on cryptology. He invented a steganographic cipher in which each letter was represented as a word taken from a succession of columns. The resulting series of words would be a legitimate prayer. He also described polyalphabetic ciphers in the now-standard form of rectangular substitution tables. He introduced the notion of changing alphabets with each letter.
1553	Civ	Kahn p.137	**Giovan Batista Belaso** introduced the notion of using a passphrase as the key for a repeated polyalphabetic cipher. (This is the standard polyalphabetic cipher operation mis-named ``Vigenère'' by most writers to this day.)
1563	Civ	Kahn p.138	**Giovanni Battista Porta** wrote a text on ciphers, introducing the digraphic cipher. He classified ciphers as transposition, substitution and symbol substitution (use of a strange alphabet). He suggested use of synonyms and misspellings to confuse the cryptanalyst. He apparently introduced the notion of a mixed alphabet in a polyalphabetic tableau.
1564	Civ	Kahn p.144(footnote)	Bellaso published an autokey cipher improving on the work of **Cardano** who appears to have invented the idea.
1623	Civ	Bacon	**Sir Francis Bacon** described a cipher which now bears his name -- a biliteral cipher, known today as a 5-bit binary encoding. He advanced it as a steganographic device -- by using variation in type face to carry each bit of the encoding. [See Bacon's writings on-line.]
1585	Civ	Kahn p.146	**Blaise de Vigenère** wrote a book on ciphers, including the first authentic plaintext and ciphertext autokey systems (in which previous plaintext or ciphertext letters are used for the current letter's key). [Kahn p.147: both of these were forgotten and re-invented late in the 19th century.] [The autokey idea survives today in the DES CBC and CFB modes.]
1790's	civ/govt	Kahn p.192, Cryptologia v.5 No.4 pp.193-208	**Thomas Jefferson**, possibly aided by **Dr. Robert Patterson** (a mathematician at U. Penn.), invented his wheel cipher. This was re-invented in several forms later and used in WW-II by the US Navy as the Strip Cipher, M-138-A.
1817	Govt	Kahn p.195	**Colonel Decius Wadsworth** produced a geared cipher disk with a different number of letters in the plain and cipher alphabets -- resulting in a progressive cipher in which alphabets are used

			irregularly, depending on the plaintext used.
1854	Civ	Kahn p.198	**Charles Wheatstone** invented what has become known as the Playfair cipher, having been publicized by his friend **Lyon Playfair**. This cipher uses a keyed array of letters to make a digraphic cipher which is easy to use in the field. He also re-invented the Wadsworth device and is known for that one.
1857	Civ	Kahn p.202	**Admiral Sir Francis Beaufort's** cipher (a variant of what's called ``Vigenère'') was published by his brother, after the admiral's death in the form of a 4x5 inch card.
1859	Civ	Kahn p.203	**Pliny Earle Chase** published the first description of a fractionating (tomographic) cipher.
1854	Civ	Cryptologia v.5 No.4 pp.193-208	**Charles Babbage** seems to have re-invented the wheel cipher.
1861-1980	Civ	Deavours	``A study of United States patents from the issuance of the first cryptographic patent in 1861 through 1980 identified 1,769 patents which are primarily related to cryptography." *[p.1]*
1861	civ/(govt)	Kahn p.207	**Friedrich W. Kasiski** published a book giving the first general solution of a polyalphabetic cipher with repeating passphrase, thus marking the end of several hundred years of strength for the polyalphabetic cipher.
1861-5	Govt	Kahn p.215	During the Civil War, possibly among other ciphers, the Union used substitution of select words followed by word columnar-transposition while the Confederacy used Vigenère (the solution of which had just been published by Kasiski).
1891	Govt/(civ)	Cryptologia v.5 No.4 pp.193-208	**Major Etienne Bazeries** did his version of the wheel cipher and published the design in 1901 after the French Army rejected it. [Even though he was a military cryptologist, the fact that he published it leads me to rate this as (civ) as well as govt.]
1913	Govt	Cryptologia v.5 No.4 pp.193-208	**Captain Parket Hitt** reinvented the wheel cipher, in strip form, leading to the M-138-A of WW-II.
1916	Govt	Cryptologia v.5 No.4 pp.193-208	**Major Joseph O. Mauborgne** put Hitt's strip cipher back in wheel form, strengthened the alphabet construction and produced what led to the M-94 cipher device.
1917	Civ	Kahn p.371	**William Frederick Friedman**, later to be honored as the father of US cryptanalysis (and the man who coined that term), was employed as a civilian cryptanalyst (along with his wife Elizebeth) at **Riverbank Laboratories** and performed cryptanalysis for the US Government, which had no

			cryptanalytic expertise of its own. WFF went on to start a school for military cryptanalysts at Riverbank -- later taking that work to Washington and leaving Riverbank.
1917	Civ	Kahn p.401	**Gilbert S. Vernam**, working for AT&T, invented a practical polyalphabetic cipher machine capable of using a key which is totally random and never repeats -- a one-time-tape. This is the only provably secure cipher, as far as we know. This machine was offered to the Government for use in WW-I but it was rejected. It was put on the commercial market in 1920.
1918	Govt	Kahn p.340-5	The ADFGVX system was put into service by the Germans near the end of WW-I. This was a cipher which performed a substitution (through a keyed array), fractionation and then transposition of the letter fractions. It was broken by the French cryptanalyst, **Lieutenant Georges Painvin**.
1919	Civ	Kahn p.420	**Hugo Alexander Koch** filed a patent in the Netherlands on a rotor based cipher machine. He assigned these patent rights in 1927 to Arthur Scherbius who invented and had been marketing the Enigma machine since about 1923.
1919	Civ	Kahn p.422	**Arvid Gerhard Damm** applied for a patent in Sweden for a mechanical rotor cipher machine. This machine grew into a family of cipher machines under the direction of **Boris Caesar Wilhelm Hagelin** who took over the business and was the only one of the commercial cryptographers of this period to make a thriving business. After the war, a Swedish law which enabled the government to appropriate inventions it felt important to defense caused Hagelin to move the company to Zug Switzerland where it was incorporated as Crypto AG. The company is still in operation, although facing controversy for having allegedly weakened a cipher product for sale to Iran.
1921	Civ	Kahn p.415	**Edward Hugh Hebern** incorporated ``Hebern Electric Code'', a company making electro-mechanical cipher machines based on rotors which turn, odometer style, with each character enciphered.
1923	Civ	Kahn p.421	**Arthur Scherbius** incorporated ``Chiffriermaschinen Aktiengesellschaft'' to make and sell his Enigma machine.
1924	Civ	Deavours p.151	**Alexander von Kryha** produced his ``coding machine'' which was used, even by the German Diplomatic Corps, into the 1950s. However, it was cryptographically weak – having a small period. A test cryptogram of 1135 characters was solved by the US cryptanalysts **Friedman, Kullback,**

			Rowlett and **Sinkov** in 2 hours and 41 minutes. Nevertheless, the machine continued to be sold and used -- a triumph of salesmanship and a lesson to consumers of cryptographic devices.
1927-33	Civ	Kahn p.802ff	Users of cryptography weren't limited to legitimate bankers, lovers, experimenters, etc. There were also a handful of criminals. ``The greatest era of international smuggling -- Prohibition -- created the greatest era of criminal cryptology.'' *[p.817]* To this day, the FBI runs a cryptanalytic office to deal with criminal cryptography. [As of Kahn's writing in 1967, that office was located at 215 Pennsylvania Avenue SE, Washington DC.] ``A retired lieutenant commander of the Royal Navy devised the systems for Consolidated Exporters' Pacific operation, though its Gulf and Atlantic groups made up their own as needed.  ``His name was unknown but his cryptologic expertise was apparent. The smugglers' systems grew increasingly more complicated. "Some of these are of a complexity never even attempted by any government for its most secret communications," wrote **Mrs. [Elizebeth Smith] Friedman** in a report in mid-1930. "At no time during the World War, when secret methods of communication reached their highest development, were there used such involved ramifications as are to be found in some of the correspondence of West Coast rum running vessels." " *[p.804]*
1929	Civ	Kahn p.404	**Lester S. Hill** published ``Cryptography in an Algebraic Alphabet'' in which a block of plaintext is enciphered by a matrix operation.
1933-45	Govt	Kahn p.422 (and many others)	The Enigma machine was not a commercial success but it was taken over and improved upon to become the cryptographic workhorse of Nazi Germany. [It was broken by the Polish mathematician, **Marian Rejewski**, based only on captured ciphertext and one list of three months worth of daily keys obtained

			through a spy. Continued breaks were based on developments during the war by **Alan Turing, Gordon Welchman** and others at Bletchley Park in England.]
1937	Govt	Kahn p.18ff.	The Japanese Purple machine was invented in response to revelations by **Herbert O. Yardley** and broken by a team headed by **William Frederick Friedman**. The Purple machine used telephone stepping relays instead of rotors and thus had a totally different permutation at each step rather than the related permutations of one rotor in different positions.
1930's	Govt	Kahn p.510ff., Deavours p.10,89-91	Kahn attributes the American SIGABA (M-134-C) to **William F. Friedman** while Deavours attributes it to an idea of **Frank Rowlett**, one of Friedman's first hires. It improved on the rotor inventions of Hebern and Scherbius by using pseudo-random stepping of multiple rotors on each enciphering step rather than have uniform, odometer-like stepping of rotors as in Enigma. It also used 15 rotors (10 for character transformation, 5 probably for controlling stepping) rather than the Enigma's 3 or 4.
1930's	Govt	Deavours p.144	The British TYPEX machine was an offshoot of the commercial Enigma purchased by the British for study in the 1920's. It was a 5-rotor machine with the two initial rotors being stators, serving the purpose of the German Enigma's plugboard.
1970	Civ	Feistel	**Dr. Horst Feistel** led a research project at the IBM Watson Research Lab in the 1960's which developed the Lucifer cipher. This later inspired the US DES (below) and other product ciphers, creating a family labeled ``Feistel ciphers''.
1976	civ/govt	FIPS PUB-46	A design by IBM, based on the Lucifer cipher and with changes (including both S-box improvements and reduction of key size) by the US NSA, was chosen to be the U.S. Data Encryption Standard. It has since found worldwide acceptance, largely because it has shown itself strong against 20 years of attacks. Even some who believe it is past its useful life use it as a component -- e.g., of 3-key triple-DES.
1976	Civ	Diffie	**Whitfield Diffie** and **Martin Hellman** published ``New Directions in Cryptography'', introducing the idea of public key cryptography. They also put forth the idea of authentication by powers of a one way function, now used in the S/Key challenge/response utility. They closed their paper with an observation for which this timeline web page gives detailed evidence: ``Skill in production cryptanalysis has always been heavily on the side of the professionals, but innovation, particularly in the design of new

			types of cryptographic systems, has come primarily from amateurs.''
April 1977	Civ	Shamir	Inspired by the Diffie-Hellman paper and acting as complete novices in cryptography, **Ronald L. Rivest, Adi Shamir** and **Leonard M. Adleman** had been discussing how to make a practical public key system. One night in April, Ron Rivest was laid up with a massive headache and the RSA algorithm came to him. He wrote it up for Shamir and Adleman and sent it to them the next morning. It was a practical public-key cipher for both confidentiality and digital signatures, based on the difficulty of factoring large numbers. They submitted this to Martin Gardner on April 4 for publication in Scientific American. It appeared in the September, 1977 issue. The Scientific American article included an offer to send the full technical report to anyone submitting a self-addressed, stamped envelope. There were thousands of such requests, from all over the world. Someone at NSA objected to the distribution of this report to foreign nationals and for a while, RS&A suspended mailings -- but when NSA failed to respond to inquiries asking for the legal basis of their request, RS&A resumed mailings. Adi Shamir believes this is the origin of the current policy [as of August 1995] that technical reports or papers can be freely distributed. [Note: two international journals, ``Cryptologia'' and ``The Journal of Cryptology'' were founded shortly after this attempt by NSA to restrain publication.] Contrary to rumor, RS&A apparently had no knowledge of ITAR or patent secrecy orders. They did not publish before applying for international patents because they wanted to avoid such restraints on free expression but rather because they were not thinking about patents for the algorithm. They just wanted to get the idea out.
1978	Civ	RSA	The **RSA** algorithm was published in the Communications of the ACM.
1984-5?	Civ	ROT13	The rot13 cipher was introduced into USENET News software to permit the encryption of postings in order to prevent innocent eyes from being assaulted by objectionable text. This is the first example I know of in which a cipher with a key everyone knows actually was effective.
1990	Civ	IACR90	**Xuejia Lai** and **James Massey** in Switzerland published ``A Proposal for a New Block Encryption Standard'', a proposed International Data Encryption Algorithm (IDEA) -- to replace DES. IDEA uses a 128-bit key and employs operations which are convenient for general purpose computers, therefore

			making software implementations more efficient.
1990	Civ	IACR90	**Charles H. Bennett, Gilles Brassard** et al. published their experimental results on Quantum Cryptography, which uses single photons to communicate a stream of key bits for some later Vernam encipherment of a message (or other uses). Assuming the laws of quantum mechanics hold, Quantum Cryptography provides not only secrecy but a positive indication of eavesdropping and a measurement of the maximum number of bits an eavesdropper might have captured. On the downside, QC currently requires a fiber-optic cable between the two parties.
1991	Civ	Garfinkel	**Phil Zimmermann** released his first version of PGP (Pretty Good Privacy) in response to the threat by the FBI to demand access to the cleartext of the communications of citizens. PGP offered high security to the general citizen and as such could have been seen as a competitor to commercial products like Mailsafe from RSADSI. However, PGP is especially notable because it was released as freeware and has become a worldwide standard as a result while its competitors of the time remain effectively unknown.
1994	Civ	Rivest	**Professor Ron Rivest**, author of the earlier RC2 and RC4 algorithms included in RSADSI's BSAFE cryptographic library, published a proposed algorithm, RC5, on the Internet. This algorithm uses data-dependent rotation as its non-linear operation and is parameterized so that the user can vary the block size, number of rounds and key length. It is still too new to have been analyzed enough to enable one to know what parameters to use for a desired strength -- although an analysis by RSA Labs, reported at CRYPTO'95, suggests that w=32, r=12 gives strength superior to DES. It should be remembered, however, that this is just a first analysis.

Sources used for above table :

- **Bacon:** Sir Francis Bacon, ``De Augmentis Scientarum'', Book 6, Chapter i. [as quoted in C. Stopes, ``Bacon-Shakspere Question'', 1889]
- **Burton:** Sir Richard F. Burton trans., ``The Kama Sutra of Vatsayana'', Arkana/Penguin, 1991.
- **Deavours:** Cipher A. Deavours and Louis Kruh, ``Machine Cryptography and Modern Cryptanalysis'', Artech House, 1985.
- **Diffie:** Whitfield Diffie and Martin Hellman, ``New Directions in Cryptography'', IEEE Transactions on Information Theory, Nov 1976.

- **Feistel:** Horst Feistel, ``Cryptographic Coding for Data-Bank Privacy'', IBM Research Report RC2827.
- **Garfinkel:** Simson Garfinkel, ``PGP: Pretty Good Privacy'', O'Reilly & Associates, Inc., 1995.
- **IACR90:** *Proceedings*, EUROCRYPT '90; Springer Verlag.
- **Kahn:** David Kahn, ``The Codebreakers'', Macmillan, 1967.
- **Price:** Derek J. Price, ``The Equatorie of the Planetis'', edited from Peterhouse MS 75.I, Cambridge University Press, 1955.
- **Rivest:** Ronald L. Rivest, ``The RC5 Encryption Algorithm'', document made available by FTP and World Wide Web, 1994.
- **ROT13:** Steve Bellovin and Marcus Ranum, individual personal communications, July 1995.
- **RSA:** Rivest, Shamir and Adleman, ``A method for obtaining digital signatures and public key cryptosystems'', Communications of the ACM, Feb. 1978, pp. 120-126.
- **Shamir:** Adi Shamir, ``Myths and Realities'', invited talk at CRYPTO '95, Santa Barbara, CA; August 1995.

Describe the History of Cryptography in the United State

CISSP Seminar :

- Herbert Yardley
- Headed first crypto unit – 1917
    - Black chamber
- Father of crypto in america
- Established foreign crypto units
    - China – 1938
    - Canada – 1941
- William Friedman
- Dean of modern American Crypto
- First Chief of Signal Intelligence Service – 1929
- Replaced Yardley’s cipher bureau
- Formed CBK
- Applied mathematics and statistical analysis
- Laurance Safford
- Developed naval communications intelligence organization

- Became Armed Forces Security Agency (AFSA – 1949)
    - NSA 1952
- Developed Underwood Code machine
- With Underwood typewriter company
- 46 Japanese-English keys
    - Copy traffic more efficiently
- Joseph Wenger
- Pioneered development of cryptanalysis machines
- Deputy director AFSA – 1949
- Vice director NSA – 1952
- Frank Rowlett
- Cryptanalysis work on machine systems
- Wheatstone device
- German Kryha machine
- The Damm machine
- Vernam's AT&T machine
- The Hebern machine
- Sigaba
    - Most secure through WWII
- Cracked Japanese Purple machine – 1940
- Verona 1943
- Project to analyze and translate encrypted Soviet message traffic (1850 translations)
- Public releases (1955-96)
- Soviet espionage against U.S. A-bomb research
- KGB, NY and Wash DC : 1944-45 messages
- KGB, San Francisco and Mexico city : 1942-46 messages
- GRU, NY and Washington : 1946 messages

- KGB and GRU, non U.S., non-mexico (e.g., Montevideo) : 1940-46 messages

Define Plaintext and Ciphertext

CISSP Seminar :
Plaintext : Data in unscrambled form
Ciphertext : Scramble data
Cryptography FAQ :
The original message is called a plaintext.
The disguised message is called a ciphertext.

Compare and contrast the terms Encipher and Decipher

CISSP Seminar :
Encipher : act of scrambling the data
Decipher : act of descrambling data with secret key
RSA Crypto FAQ :
Encryption (Encipher) is the transformation of data into a form that is as close to impossible as possible to read with out the appropriate knowledge (a key). Its purpose is to ensure privacy by keeping information hidden from anyone for whom it is not intended, even those who have access to the encrypted data.
Decryption (Decipher) is the reverse of encryption; it is the transformation of encrypted data back into an intelligible form.
Encryption and decryption generally require the use of some secret information, referred to as a key. For some encryption mechanisms, the same key is used for both encryption and decryption; for other mechanisms, the keys used for encryption and decryption are different

Define Cryptanalysis

CISSP Seminar :
Cryptanalysis : Descrambling without secret key
RSA Crypto FAQ :
Cryptanalysis is the flip-side of cryptography: it is the science of cracking codes, decoding secrets, violating authentication schemes, and in general, breaking cryptographic protocols.
In order to design a robust encryption algorithm or cryptographic protocol, one should use cryptanalysis to find and correct any weaknesses. This is precisely the reason why the best (most trusted) encryption algorithms are ones that have been made available to public scrutiny. For example, DES has been exposed to public scrutiny for years, and is therefore well-trusted, while Skipjack is secret and less well-trusted. It is a basic tenet of cryptology that the security of an algorithm should not rely on its secrecy. Inevitably, the algorithm will be discovered and its weaknesses (if any) will be exploited.

The various techniques in cryptanalysis attempting to compromise cryptosystems are referred to as attacks. Some attacks are general, whereas others apply only to certain types of cryptosystems.

Define "Key" as it refer to Cryptography

CISSP Seminar:

Key: Secret sequence governing en/deciphering

RSA Crypto FAQ:

A cryptosystem is usually a whole collection of algorithms. The algorithms are labelled; the labels are called keys. For instance, Caesar probably used ``shift by n'' encryption for several different values of n. It's natural to say that **n** is the **key** here.

Define the Strength of key as it pertains to key length

CISSP Seminar:

Considering that encryption is based on factoring factor, a longer key will provide better protection than a shorter key. However one must ensure that the algorithm being used is a strong cryptosystem.

Consider the following from the Cryptography FAQ:

Every well-designed cryptosystem has such a large key space that this brute-force search is impractical.

Advances in technology sometimes change what is considered practical. For example, DES, which has been in use for over 10 years now, has 2^56, or about 10^17, possible keys. A computation with this many operations was certainly unlikely for most users in the mid-70's. The situation is very different today given the dramatic decrease in cost per processor operation. Massively parallel machines threaten the security of DES against brute force search.

RSA Crypto FAQ:

The security of a strong system resides with the secrecy of the key rather than with the supposed secrecy of the algorithm.

A strong cryptosystem has a large keyspace. It has a reasonably large unicity distance.

The unicity distance is an approximation to that amount of ciphertext such that the sum of the real information (entropy) in the corresponding source text and encryption key equals the number of ciphertext bits used. Ciphertexts significantly longer than this can be shown probably to have a unique decipherment. This is used to back up a claim of the validity of a ciphertext-only cryptanalysis. Ciphertexts significantly shorter than this are likely to have multiple, equally valid decryptions and therefore to gain security from the opponent's difficulty choosing the correct one.

Define Ciphertext Only Attack (COA)

CISSP Seminar:

Only statistical knowledge of plaintext available.

RSA Crypto FAQ:

A ciphertext-only attack is one in which the cryptanalyst obtains a sample of ciphertext, without the plaintext associated with it. This data is relatively easy to obtain in many scenarios, but a successful ciphertext-only attack is generally difficult, and requires a very large ciphertext sample.

Define known Plaintext Attact (KPA)

CISSP Seminar:
Some past plain text and matching ciphertext known
RSA Crypto FAQ:
A known-plaintext attack is one in which the cryptanalyst obtains a sample of ciphertext and the corresponding plaintext as well.

Define Chosen Text Attack (CTA)

CISSP Seminar:
Crypto device loaded with hidden key provided and input of plaintext or ciphertext allowed to see the other.
RSA Crypto FAQ:
A chosen-plaintext attack is one in which the cryptanalyst is able to choose a quantity of plaintext and then obtain the corresponding encrypted ciphertext.

Describe Stream Ciphers

CISSP Seminar:
Operate on continuous streams of plain text (as 1's and 0's)
Usually implemented in hardware
RSA Crypto FAQ:
A stream cipher is a type of symmetric encryption algorithm. Stream ciphers can be designed to be exceptionally fast, much faster than any block cipher. While block ciphers operate on large blocks of data, stream ciphers typically operate on smaller units of plaintext, usually bits. The encryption of any particular plaintext with a block cipher will result in the same ciphertext when the same key is used. With a stream cipher, the transformation of these smaller plaintext units will vary, depending on when they are encountered during the encryption process. A stream cipher generates what is called a keystream (a sequence of bits used as a key). Encryption is accomplished by combining the keystream with the plaintext, usually with the bitwise exclusive-OR operation. The generation of the keystream can be independent of the plaintext and ciphertext (yielding what is termed a synchronous stream cipher) or it can depend on the data and its encryption (in which case the stream cipher is said to be self-synchronizing). Most stream cipher designs are for synchronous stream ciphers.

Define Block Ciphers

CISSP Seminar:
Operate on fixed size blocks of plain text

More suitable implemented in software to execute on general-purpose computer
There is some overlap when block operated as stream.
RSA Crypto FAQ:
A block cipher is a type of symmetric-key encryption algorithm that transforms a fixed-length block of plaintext (unencrypted text) data into a block of ciphertext (encrypted text) data of the same length. This transformation takes place under the action of a user-provided secret key. Decryption is performed by applying the reverse transformation to the ciphertext block using the same secret key. The fixed length is called the block size, and for many block ciphers, the block size is 64 bits. In the coming years the block size will increase to 128 bits as processors become more sophisticated.

Describe Features of Stream Cipher Algorithm

CISSP Seminar:
Long periods of time with no repeating
Functionally complex
Statistically unpredictable
Statistically unbiased keystream
As many 0's and 1's
Keystream not linearly related to key

Identify the Applications of Cryptography

CISSP Seminar:

- Data Storage
- Prevent disclosure
- Password files
- Backup tapes
- Bulk
- Telecommunications
- Prevent disclosure
- Data transmission
- STU
- Message authentication
- Detect fraudulent insertion
- Detect fraudulent deletion
- Detect fraudulent modification

- Detect replay
- Digital Signature
- Source Verification
- Non-Repudiation

RSA Crypto FAQ :

A typical application of cryptography is a system built out of the basic techniques. Such systems can be of various levels of complexity. Some of the more simple applications are secure communication, identification, authentication, and secret sharing. More complicated applications include systems for electronic commerce, certification, secure electronic mail, key recovery, and secure computer access. In general, the less complex the application, the more quickly it becomes a reality. Identification and authentication schemes exist widely, while electronic commerce systems are just beginning to be established.

Secure Communication

Secure communication is the most straightforward use of cryptography. Two people may communicate securely by encrypting the messages sent between them. This can be done in such a way that a third party eavesdropping may never be able to decipher the messages. While secure communication has existed for centuries, the key management problem has prevented it from becoming commonplace. Thanks to the development of public-key cryptography, the tools exist to create a large-scale network of people who can communicate securely with one another even if they had never communicated before.

Identification and Authentication

Identification and authentication are two widely used applications of cryptography. Identification is the process of verifying someone's or something's identity. For example, when withdrawing money from a bank, a teller asks to see identification (e.g. a driver's license) to verify the identity of the owner of the account. This same process can be done electronically using cryptography. Every automatic teller machine (ATM) card is associated with a "secret" personal identification number (PIN), which binds the owner to the card and thus to the account. When the card is inserted into the ATM, the machine prompts the cardholder for the PIN. If the correct PIN is entered, the machine identifies that person as the rightful owner and grants access. Another important application of cryptography is authentication. Authentication is similar to identification, in that both allow an entity access to resources (such as an Internet account), but authentication is broader because it does not necessarily involve identifying a person or entity. Authentication merely determines whether that person or entity is authorized for whatever is in question. For more information on authentication and identification.

Secret Sharing

Another application of cryptography, called secret sharing, allows the trust of a secret to be distributed among a group of people. For example, in a (K, N)-threshold scheme, information about a secret is distributed in such a way that any K out of the N people (K<N) have enough information to determine the secret, but any set of K-1 people do not. In any secret sharing scheme, there are designated sets of people whose cumulative information suffices to determine the secret. In some implementations of secret sharing schemes, each participant receives the secret after it has been generated. In other implementations, the actual secret is never made visible to the participants, although the purpose for which they sought the secret (e.g. access to a building or permission to execute a process) is allowed.

Electronic Commerce

Over the past few years there has been a growing amount of business conducted over the Internet - this form of business is called electronic commerce or e-commerce. E-commerce is comprised of online banking, online brokerage accounts, and Internet shopping, to name a few of the many applications. One can book plane tickets, make hotel reservations, rent a car, transfer money from one account to another, buy compact disks (CDs), clothes, books and so on all while sitting in front of a computer. However, simply entering a credit card number on the Internet leaves one open to fraud. One cryptographic solution to this problem is to encrypt the credit card number (or other private information) when it is entered on-line, another is to secure the entire session. When a computer encrypts this information and sends it out on the Internet, it is incomprehensible to a third party viewer. The web-server ("Internet shopping center") receives the encrypted information, decrypts it, and proceeds with the sale without fear that the credit card number (or other personal information) slipped into the wrong hands. As more and more business is conducted over the Internet, the need for protection against fraud, theft and corruption of vital information increases.

Certification

Another application of cryptography is certification; certification is a scheme by which trusted agents such as certifying authorities vouch for unknown agents, such as users. The trusted agents issue vouchers called certificates which each have some inherent meaning. Certification technology was developed to make identification and authentication possible on a large scale.

Key Recovery

Key recovery is a technology that allows a key to be revealed under certain circumstances without the owner of the key revealing it. This is useful for two main reasons: first of all, if a user loses or accidentally deletes their key, key recovery could prevent a disaster. Secondly, if a law enforcement agency wishes to eavesdrop on a suspected criminal without their knowledge (akin to a wiretap), they must be able to recover the key. Key recovery techniques are in use in some instances; however, the use of key recovery as a law enforcement technique is somewhat controversial.

Remote Access

Secure remote access is another important application of cryptography. The basic system of passwords certainly gives a level of security for secure access, but it may not be enough in some cases. For instance, passwords can be eavesdropped, forgotten, stolen, or guessed. Many products supply cryptographic methods for remote access with a higher degree of security.

Other Applications

Cryptography is not confined to the world of computers. Cryptography is also used in cellular phones as a means of authentication; that is, it can be used to verify that a particular phone has the right to bill to a particular phone number. This prevents people from stealing ("cloning") cellular phone numbers and access codes.

Identify the Uses of Cryptography

CISSP Seminar:

- EFT systems
- E-Mail
- Communication links

RSA Crypto FAQ:

Today's cryptography is more than encryption and decryption. Authentication is as fundamentally a part of our lives as privacy. We use authentication throughout our everyday lives -when we sign our name to some document for instance and, as we move to a world where our decisions and agreements are communicated electronically, we need to have electronic techniques for providing authentication.

Cryptography provides mechanisms for such procedures. A digital signature binds a document to the possessor of a particular key, while a digital timestamp binds a document to its creation at a particular time. These cryptographic mechanisms can be used to control access to a shared disk drive, a high security installation, or a pay-per-view TV channel.

The field of cryptography encompasses other uses as well. With just a few basic cryptographic tools, it is possible to build elaborate schemes and protocols that allow us to pay using electronic money, to prove we know certain information without revealing the information itself, and to share a secret quantity in such a way that a subset of the shares can reconstruct the secret.

Compare and contrast Symmetric and Asymmetric Key Cryptography

CISSP Seminar:

SYMMETRIC KEY:

- Also known as private key, single key, secret key
- Key shared by originator and receiver
- Computational efficiency advantage

- 1-100 million bits/sec.
- Data Encryption Standard (DES)

ASYMMETRIC KEY:

- Also known as public key
- Uses 2 asymmetric keys
- One to encrypt and one to decrypt
- Computationnally slow
- Few thousand bits/sec. (early versions)
- Rivest-Shamir-Adleman (RSA) algorithm
- Related to known mathematical problem
- Difficulty factoring product of 2 large prime numbers

RSA Crypto FAQ:

There are two types of cryptosystems: secret-key and public-key.

In secret-key cryptography, also referred to as symmetric cryptography, the same key is used for both encryption and decryption. The most popular secret-key cryptosystem in use today is known as DES, the Data Encryption Standard. IBM developed DES in the middle 1970's and it has been a Federal Standard ever since 1976.

In public-key cryptography, each user has a public key and a private key. The public key is made public while the private key remains secret. Encryption is performed with the public key while decryption is done with the private key. The RSA public-key cryptosystem is the most popular form of public-key cryptography. RSA stands for Rivest, Shamir, and Adleman, the inventors of the RSA cryptosystem.

The Digital Signature Algorithm (DSA) is also a popular public-key technique, though it can only be used only for signatures, not encryption.

The primary advantage of public-key cryptography is increased security and convenience: private keys never need to be transmitted or revealed to anyone. In a secret-key system, by contrast, the secret keys must be transmitted (either manually or through a communication channel) since the same key is used for encryption and decryption. A serious concern is that there may be a chance that an enemy can discover the secret key during transmission.

Another major advantage of public-key systems is they can provide digital signatures that cannot be repudiated. Authentication via secret-key systems requires the sharing of some secret and sometimes requires trust of a third party as well. As a result, a sender can repudiate a previously authenticated message by claiming the shared secret was somehow compromised by one of the parties sharing the secret. For example, the Kerberos secret-key authentication system

involves a central database that keeps copies of the secret keys of all users; an attack on the database would allow widespread forgery. Public-key authentication, on the other hand, prevents this type of repudiation; each user has sole responsibility for protecting his or her private-key. This property of public-key authentication is often called non-repudiation.
A disadvantage of using public-key cryptography for encryption is speed. There are many secret-key encryption methods that are significantly faster than any currently available public-key encryption method. Nevertheless, public-key cryptography can be used with secret-key cryptography to get the best of both worlds. For encryption, the best solution is to combine public and secret-key systems in order to get both the security advantages of public-key systems and the speed advantages of secret-key systems. Such a protocol is called a digital envelope.
Public-key cryptography may be vulnerable to impersonation, even if users' private-keys are not available. A successful attack on a certification authority will allow an adversary to impersonate whomever he or she chooses by using a public-key certificate from the compromised authority to bind a key of the adversary's choice to the name of another user.
In some situations, public-key cryptography is not necessary and secret-key cryptography alone is sufficient. These include environments where secure secret key distribution can take place, for example, by users meeting in private. It also includes environments where a single authority knows and manages all the keys, e.g., a closed banking system. Since the authority knows everyone's keys already, there is not much advantage for some to be "public" and others "private." Also, public-key cryptography is usually not necessary in a single-user environment. For example, if you want to keep your personal files encrypted, you can do so with any secret-key encryption algorithm using, say, your personal password as the secret key. In general, public-key cryptography is best suited for an open multi-user environment.
Public-key cryptography is not meant to replace secret-key cryptography, but rather to supplement it, to make it more secure. The first use of public-key techniques was for secure key establishment in a secret-key system [DH76]; this is still one of its primary functions. Secret-key cryptography remains extremely important and is the subject of much ongoing study and research.

Identify Types of Encryption Systems

CISSP Seminar:

- Classical substitution ciphers
- Transposition (permutation) ciphers
- Polyalphabetic Ciphers
- Running key ciphers

- Concealment
- Digital System
- Codes
- Machines
- One-Time pad
- DES/Clipper
- Double/Triple DES
- Public Key
- RSA
- Elliptic curve
- PGP
- El Gamal
- Diffie-Hellman

Compare and contrast Substitution ciphers and Transposition Ciphers

CISSP Seminar:

An example of substitution cipher would be the ‘’Ceasar cipher’’. In which each plaintext character is replaced by the character three to the right of modulo 26 (‘’A’’ is replaced by ‘’D’’, ‘’B’’ is replaced by ‘’E’’, and so on…

Shift alphabet Example:

```
A B C D E F…. BAD
D E F G H I…… EDG
```

Scramble Alphabet Example:

```
A B C D E F…. BAD
Q E Y R T M…. EQR
```

An example of transposition cipher would be as follows:

- Position of letters permuted.
- Message broken into 5-character groups
- Letters rearranged

```
don’t give up the ship (Message)
123451234512345123451234512345 (Groups of 5)
351243512435124351243512435124 (The key)
n’dtoiv egp tu shhe i p (Ciphertext)
```

RSA Crypto FAQ:

A substitution cipher is one in which each character of the plaintext is substituted for another character of ciphertext. The receiver inverts the substitution on the ciphertext to recover the plaintext.
In a Transposition cipher the plaintext remains the same, but the order of characters is shuffled around.

Describe the concept of Polyalphabetic Ciphers

CISSP Seminar:
Uses different alphabets to defeat frequency analysis.

- See example with 5 alphabets below

Example:
a b c d e f g h i (normal alphabet)
q w e r t……. (1st alphabet)
d m s i k …… (2nd Alphabet)
o h g x f…… (3rd Alphabet)
z b n l a …… (4th Alphabet)
y c v u p …… (5th Alphabet)
abcde (Plaintext)
qdozy (ciphertext)
Applied Cryptography bood, Page 10:
A polyalphabetic cipher is made up of multiple simple substitution cipher. For example, there might be five different simple substitution cipher used; the particular one used changes with the position of each character of the plaintext.

Describe the concept of Concealment Ciphers

CISSP Seminar:
The true letters of plaintext are hidden/disguised

- By device or algorithm
- Example: divide message
    - Use 1 word at a time
    - Have it appear as every 5th word in a sentence
    - Message in clear text: ‘’Buy gold’’
    - Message in concealment:
      ‘’Product is a good BUY, it has ten percent GOLD content’’

Define and describe Steganography

CISSP Seminar:
Stenography is the art of hiding communications

- Deny message exists

- Data hidden in picture files, sound files, slack space on floppies
    - I:e Least significant bits of Bitmap image can be used to hide messages, usually without material change to original file.

Applied Cryptography, Page 9:
Steganography serves to hide secret messages in other messages, such that the secret's very existence is concealed. Generally the sender writes an innocuous message and then conceals a secret message on the same piece of paper. Historical tricks includes invisible inks, tiny pin puncture on selected characters, minute differences between handwritten characters, pencil marks on typewritten characters, grilles which cover most of the message except for a few characters, and so on. More recently people are hiding secrets in graphic image.

Describe Digital System Encryption

CISSP Seminar:
The key and message both streams of bits

- Each text character = 8 bits
- Each key bit XORed (exclusived-or'ed) with corresponding message bit
- XOR operation yields 0 if both bits the same and 1 is different

Example:
MESSAGE STREAM 01001000
KEY STREAM 11010001
CIPHERTEXT STREAM 10011001

Define the word "Codes" as it pertains to Cryptography

CISSP Seminar:
List of words/phrases/ (codes) with corresponding random groups of numbers/letters (code groups)
Applied Cryptography, Page 9:
Historically, a code refers to a cryptosystem that deals with linguistic units: words, phrases, sentences, and so forth. For example, the word ''OCELOT'' might be the ciphertext of the entire phrase ''Turn left 90 degrees'', the word ''LOLLIPOP'' might be the ciphertext for ''Turn right 90 degrees'', and the words ''BENT EAR'' might be the ciphertext for ''HOWITZER''. Codes are only useful for specialized circumstances. Ciphers are useful for any circumstance. Codes are limited, if your code does not have an entry for a specific word then you can't say it, you can say anything you wish using cipher.

Compare and contrast Hagelin and Rotor Cryptography Machines

CISSP Seminar:

- Hagelin Machine

- Combines plain text (character by character) with:
- Keystream (long pseudo-random sequence)
- To produce cipher text
- Rotor Machines
- Rotor implements cipher alphabet
- Rotor connected in banks
- Signal entering one end permuted by each of rotors before leaving at other end
- Keyed by changing rotor variables
    - Rotors/order of rotors
    - Number of stopping pieces per wheel
    - Pattern of motion

Describe the use and characteristics of "One-Time-Pad" Encryption

CISSP Seminar:

- Unbreakable by exhaustive search (brute force)
- Random key same length as message
- Only used once
- Digital system key and message both bit streams
- 8 bits per character
- Each key bit XORed with corresponding message bit
- Produces ciphertext bit
- Key bits XORed with ciphertext to decrypt

Describe the history of the DES Encryption

CISSP Seminar:

- IBM cryptographic research (late 1960's)
- Modification of Lucifer developed by IBM
- Non-linear block ciphers
- IBM developed (about 1972)

- NBS solucited (about 1973 and 1974)
- Adopted (1977)
- ANSI approved (1978)
- NSA threatened decertification (1987)
- NIST recertified for 5 years (1988, 1993)

Network Computing:
The most common private key encryption standard that is used is the Data Encryption Standard (DES) developed by IBM in the early 1970s. It is the de facto industry standard for cryptography systems and is the world's most commonly used encryption mechanism. This private key system is widely deployed in financial networks including automated teller machines and point-of-sale networks. It was adopted as a Federal Information Processing Standard (FIPS PUB 46) in 1977 and as an American National Standard (ANSI X3.92) in 1981. Further clarification on the modes of use of the algorithm is contained in ANSI standard X3.106.

Describe the DES Algorithm

CISSP Seminar:

- 64 bit plain and cipher text block size
- 56 bit true key plus 8 parity bits
- Seventy quadrillion possible keys
- Single-Chip LSI implentation
- About 50$ per unit
- 16 rounds of simple operations to encrypt
- Transposition and substitution
- Reverse to decrypt

RSA Crypto FAQ:
The DEA, also called DES, has been extensively studied since its publication and is the best known and widely used symmetric algorithm in the world.
The DEA has a 64-bit block size and uses a 56-bit key during execution (8 parity bits are stripped off from the full 64-bit key). The DEA is a symmetric cryptosystem, specifically a 16-round Feistel cipher and was originally designed for implementation in hardware. When used for communication, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message, or to generate and verify a message authentication code (MAC). The DEA can also be used for single-user encryption, such as to store

files on a hard disk in encrypted form. In a multi-user environment, secure key distribution may be difficult; public-key cryptography provides an ideal solution to this problem.
NIST has recertified DES (FIPS 46-1) every five years; DES was last recertified in 1993, by default. NIST has indicated, however, it will not recertify DES again. The development of AES, the Advanced Encryption Standard is underway. AES will replace DES.

Compare and contrast the Modes of the DES Algorithm

CISSP Seminar:

- Electronic code book
- 64 bits data blocks entered directly into device
- 64 bits cipher blocks generated under key
- Restricted to protection of encrypting keys and initializing vectors
- Output Feedback
- DES generated keystream XORed with message stream
- Simulates one-time-pad
- Keystream generated by DES encrypting 64 bits initialization vector with secret key
- DES output bits fed back as input to generate next segment key bits
- Cipher Feedback
- Device generates stream of random binary bits
- Combined with plain text
- Generated cipher with same number of bits as text
- Cipher text fed back to form a portion of next input
- Cipher Block Chaining
- 64 bit plain text blocks loaded sequentially
- XORed with 64 bits initializing vector
- Combination processed into cipher under key
- First ciphertext XORed with next text block
- Process continues until end of plaintext chain

RSA Crypto FAQ:

ECB - Electronic Code Book
Each block of ciphertext is encrypted independently of any other block. Therefore each ciphertext block corresponds to one plaintext block just like in a code book.
CBC - Chain Block Cipher
ECB does not protect against insertion of repeated blocks because blocks are treated independently. Another weakness is that identical plaintext blocks generate identical ciphertext blocks. To improve DES for communication streams each 64 bit block is EXORed with the previous 64 bit ciphertext before entered into the DES chip. In addition to a common secret key the sender and receiver need to agree on an initial vector to be EXORed with the first block of a messages stream.
CFM - Cipher Feedback Mode
CFM is an alternate mode for DES on 8 bit characters. The input character is EXORed with the least significant byte of the DES output and then transmitted over the
communication link. In order to collect enough bits for the 64 bit encryption block the output characters are collected in a character based shift register. Each output character advances the shift register by 8 bits and triggers a new DES encryption. Thereby the next input character will be EXORed with a new DES output. CFM is suitable for use on serial lines.

Describe the caracteristics and usage of Double/Triple DES

CISSP Seminar:

- Double DES
- Effective key length 112 bits
- Work factor about the same as single DES
- No more secure
- Triple DES
- Encrypt with first key
- Decrypt with second key
- Encrypt with first key
- No successfull attack reported

RSA Crypto FAQ:
For some time it has been common practice to protect and transport a key for DES encryption with triple-DES. This means that the input data (in this case the single-DES key) is, in effect encrypted three times. There are of course a variety of ways of doing this; we will explore these ways below.
A number of modes of triple-encryption have been proposed:

DES-EEE3: Three DES encryptions with three different keys.
DES-EDE3:
Three DES operations in the sequence encrypt-decrypt-encrypt with three different keys.
DES-EEE2 and DES-EDE2:
Same as the previous formats except that the first and third operations use the same key.
Attacks on two-key triple-DES have been proposed by Merkle and Hellman [MH81] and Van Oorschot and Wiener [VW91], but the data requirements of these attacks make them impractical. Further information on triple-DES can be obtained from various sources [Bih95][KR96].
The use of double and triple encryption does not always provide the additional security that might be expected. Preneel [Pre94] provides the following comparisons in the security of various versions of multiple-DES and it can be seen that the most secure form of multiple encryption is triple-DES with three distinct keys.

# Encryptions	#Keys	Computation	Storage	Type of attack
single	1	2^56	-	known plaintext
single	1	2^38	2^38	chosen plaintext
single	1	-	2^56	chosen plaintext
double	2	2^112	-	known plaintext
double	2	2^56	2^56	known plaintext
double	2	-	2^112	known plaintext
triple	2	2^56	2^56	2^56 known plaintext
triple	2	2^120-t	2t	2t known plaintext
triple	2	-	2^56	chosen plaintext
triple	3	2^112	2^56	known plaintext
triple	3	2^56	2^112	chosen plaintext

Table 1: Comparison of different forms of DES multiple encryption
Like all block ciphers, triple-DES can be used in a variety of modes. The ANSI X9.52 standard (see Question 5.3.1) details the different ways in which triple-DES might be used and is expected to be completed during 1998.

Compare and Contrast the Relative Benefits of Escrowed Encryption

CISSP Seminar:
To be completed????
Personal comments:
Key escrow is a real can of worm depending on who you are talking to.
There is two side of this, a group that claim it is madatory and another group that claim it would be against their freedom of speech and civil liberties.
Here are some of the degates:
Criminal encryption use exists. Encryption has already been used by criminals to keep their activities secret from the FBI and law enforcement. From 1995 to 1996, the number of cases in which the FBI was foiled by encryption more than doubled (5 to 12).

Encryption is not regulatable outside the US. Non-escrowed strong encryption is already available in over 200 other countries, and it will still be available in these countries, even if the US Government decides to institute an escrowed encryption policy.
Key recovery is expensive. A mandatory key recovery policy, if instituted by the government, would be very costly not only for the government itself (operational costs), but also for software companies that have developed the 800 encryption products currently on the market. These companies will have to completely re-engineer their products in order to comply with the government's new policy.
Escrow has not been thoroughly tested. There are millions of encryption users and thousands of agents and law enforcement agencies. Key escrow has never been tested in a wide-scale environment.
Mandatory escrow can be circumvented. There is no way to "scan" the Internet to detect use of non-escrowed encryption. Key recovery leaves a "back door" in the software. Our nation's critical systems (air traffic control, defense systems, the power grid, etc.) would likely be protected by key recovery. There is no way to ensure that the system will be safe from hackers and terrorists.
Escrow involves humans. As with any type of security system involving humans, there are vulnerabilities.
The government would hold the key to everyone's personal data. Under current proposed legislation, keys would be released by a court subpoena, not a judicial order.

Define "Clipper" and the "Shipjack" Algorithm

CISSP Seminar:

- Clipper
- Tamper-resistant hardware chip
- NSA-designed single-key encryption algorithm (shipjack)
- Decrypted by special chip, unique key and special law enforcement access field (LEAF) transmitted with encrypted communication.
- Regardless of session key
- Chip unique key is XOR of 2 components
- Each encrypted and stored in escrow with separate escrow agent
- Both needed to construct chip unique key and decrypt
- Release to authorized government agent for authorized surveillance.
- Shipjack Algorithm
- Transform 64 bit input block into 64 bit output block

- 80 bit key length
- Same operating modes as DES (4 of them)
- Classified to prevent implementing (in either software or hardware) without LEAF

RSA Crypto FAQ:
The Clipper chip contains an encryption algorithm called Skipjack. Each chip contains a unique 80-bit unit key U, which is escrowed in two parts at two escrow agencies; both parts must be known in order to recover the key. Also present is a serial number and an 80-bit "family key" F; the latter is common to all Clipper chips. The chip is manufactured so that it cannot be reverse engineered; this means that the Skipjack algorithm and the keys cannot be recovered from the chip.
Skipjack is the encryption algorithm contained in the Clipper chip, designed by the NSA (see Question 6.2.2). It uses an 80-bit key to encrypt 64-bit blocks of data. Skipjack is expected to be more secure than DES in the absence of any analytic attack since it uses 80-bit keys. By contrast, DES uses 56-bit keys.
Initially the details of Skipjack were classified and the decision not to make the details of the algorithm publicly available was widely criticized. Some people were suspicious that Skipjack might not be secure, either due to an oversight by its designers, or by the deliberate introduction of a secret trapdoor. Since Skipjack was not public, it could not be widely scrutinized and there was little public confidence in the cipher.
Aware of such criticism, the government invited a small group of independent cryptographers to examine the Skipjack algorithm. They issued a report [BDK93] which stated that although their study was too limited to reach a definitive conclusion, they nevertheless believed Skipjack was secure.
In June of 1998 Skipjack was declassified by the NSA. Early cryptanalysis has failed to find any substantial weakness in the cipher.

Describe the elements of the Electronic Data Security Act of 1997

CISSP Seminar:
To be completed????
Electronic Data Security Act 1997:
The Electronic Data Security Act states it’s goals as:
To enable the development of a key management infrastructure for public-key-based encryption and attendant encryption products that will assure that individuals and businesses can transmit and receive information electronically with confidence in the information's confidentiality, integrity, availability, and authenticity, and that will promote timely lawful government access.

Describe the basis of Public-Key Algorithms

CISSP Seminar:

- Factoring large prime numbers
- RSA
- Discrete log problem (difficulty of taking logarithms in finite fields)
- El Gamal encryption scheme and signature algorithm
- Schnorr's signature algorithm
- Nybergrueppel's signature algorithm
- Station-to-Station protocol for key agreement (STS)
- Digital Signature Algorithm (DSA)
- Elliptic Curve Crypto (ECC)

RSA Crypto FAQ:
Public-key cryptosystems are based on a problem that is in some sense difficult to solve. Difficult in this case refers more to the computational requirements in finding a solution than the conception of the problem. These problems are called hard problems. Some of the most well known examples are factoring, theorem-proving, and the "traveling salesman problem" - finding the route through a given collection of cities which minimizes the total length of the path.
Factoring is the underlying, presumably hard problem upon which several public-key cryptosystems are based, including the RSA algorithm. Factoring an RSA modulus would allow an attacker to figure out the private key; thus, anyone who can factor the modulus can decrypt messages and forge signatures. The security of the RSA algorithm depends on the factoring problem being difficult and the presence of no other types of attack.
In general the larger the number the more time it takes to factor it. Of course if you have a number like 2^100 it is easier to factor than say, a number with half as many digits but the product of two primes of about the same length. This is why the size of the modulus in RSA determines how secure an actual use of RSA is; the larger the modulus, the longer it would take an attacker to factor, and thus the more resistant the RSA modulus is to an attack.

Define Elleptic Curve Cryptosystems (ECC)

CISSP Seminar:

- Uses algebraic system defined on points of elliptic curve to provide public-key algorithms.
- Digital signature
- Secret key distribution
- Confidential info transmission

- First proposed by Victor Miller (IBM/CRD) 1985 & Neal koblitz (Washington univ)

RSA Crypto FAQ:
Elliptic curve cryptosystems were first proposed independently by Victor Miller [Mil86] and Neal Koblitz [Kob87] in the mid-1980s. At a high level, they are analogs of existing public-key cryptosystems in which modular arithmetic is replaced by operations defined over elliptic curves. The elliptic curve cryptosystems that have appeared in the literature can be classified into two categories according to whether they are analogs to RSA or discrete logarithm based systems.

Describe the advantages of Elliptic Curves Cryptosystems (ECC)

CISSP Seminar:

- Highest strength/bit of public key systems
- Big saving over other public key systems
- Computation
- Bandwidth
- Storage
- Bandwith reduced
- Short signature and certificates
- Fast encryption and signature speed
- Hardware and software
- Ideal for very small hardware implementations
- Smart card
- Encryption and digital signatures stages separable to simplify export

RSA Crypto FAQ:
Presently, the methods for computing general elliptic curve discrete logs are much less efficient than those for factoring or computing conventional discrete logs. As a result, shorter key sizes can be used to achieve the same security of conventional public-key cryptosystems, which might lead to better memory requirements and improved performance. One can easily construct elliptic curve encryption, signature, and key agreement schemes by making analogs of ElGamal, DSA, and Diffie-Hellman. These variants appear to offer certain implementation advantages over the original schemes, and they have recently

drawn more and more attention from both the academic community and the industry.
The main attraction of elliptic curve cryptosystems over other public-key cryptosystems is the fact that they are based on a different, hard problem. This may lead to smaller key sizes and better performance in certain public-key operations for the same level of security.
Very roughly speaking, when this FAQ was published elliptic curve cryptosystems with a 160-bit key offer the same security of RSA and discrete logarithm based systems with a 1024-bit key. As a result, the length of the public key and private key is much shorter in elliptic curve cryptosystems. In terms of speed, however, it is quite difficult to give a quantitative comparison, partly because of the various optimization techniques one can apply to different systems. It is perhaps fair to say the following: Elliptic curve cryptosystems are faster than the corresponding discrete logarithm based systems. Elliptic curve cryptosystems are faster than RSA in signing and decryption, but slower than RSA in signature verification and encryption. For more detailed comparisons, see the survey article by Matt Robshaw and Yiqun Lisa Yin [RY97].
With academic advances in attacking different hard mathematical problems both the security estimates for various key sizes in different systems and the performance comparisons between systems are likely to change.

Identify the standards Activities Involving Elliptic Curve Cryptosystems (ECC)

CISSP Seminar:

- IEEE, P1363 (public-key crypto)
- Covers main public key techniques
- RSA, ECC, El Gamal, Diffie-Hellman
- ANSI X9
- Elliptic curve Digital Signature Algorithm
- (ECDSA) proposed work item
- ANSI ASC X9
- Elliptic curve key agreement and key management proposed work item
- ISO/IEC CD 148883 "Digital Signature with appendix"
- Variety of digital signature mechanisms

RSA Crypto FAQ:

The IEEE P1363 is an emerging standard that aims to provide a comprehensive coverage of established public-key techniques. It continues to move toward completion, with balloting expected later this year. The project, begun in 1993, has produced a draft standard covering public-key techniques from the discrete logarithm, elliptic curve, and integer factorization families. Contributions are currently solicited for an addendum, IEEE P1363a, which will cover additional public-key techniques. The project is closely coordinated with emerging ANSI standards for public-key cryptography in banking, and forthcoming revisions of RSA Laboratories' Public-Key Cryptography Standards will also be aligned with IEEE P1363.
American National Standards Institute (ANSI) is broken down into committees, one being ANSI X9. The committee ANSI X9 develops standards for the financial industry, more specifically for personal identification number (PIN) management, check processing, electronic transfer of funds, etc. Within the committee of X9, there are subcommittees; further broken down are the actual documents, such as X9.9 and X9.17.
The International Organization for Standardization, (ISO), is a non-governmental body promoting standardization developments globally. Altogether, ISO is broken down into about 2700 Technical Committees, subcommittees and working groups. ISO/IEC (International Electrotechnical Commission) is the joint technical committee developing the standards for information technology. One of the more important information technology standards developed by ISO/IEC is ISO/IEC 9798 [ISO92a]. This is an emerging international standard for entity authentication techniques. It consists of five parts. Part 1 is introductory, and Parts 2 and 3 define protocols for entity authentication using secret-key techniques and public-key techniques. Part 4 defines protocols based on cryptographic checksums, and part 5 addresses zero-knowledge techniques.

Describe Pretty Good Privacy (PGP)

CISSP Seminar:

- Created by Phil Zimmerman
- Random prime number + pass phrase
- Key crunching generates key
- Convert passphrase into bitsteam
- For random key, passphrase must be long
    - Theory: number of passphrase characters = numbers of bits in key

RSA Crypto FAQ:
PGP (Pretty Good Privacy) is a software package originally developed by Phil Zimmerman that provides cryptographic routines for e-mail, file transfer, and file storage applications. Zimmerman used existing cryptographic algorithms and

protocols and developed a system that can run on multiple platforms. It provides message encryption, digital signatures, data compression, and e-mail compatibility.
The algorithms used by PGP have changed over its various versions. Versions prior to 5.0 used RSA for key exchange, MD5 for digital signatures, and IDEA for bulk encryption of messages and files. Version 5.0 added Diffie-Hellman (El Gamal) for key exchange, RIPEMD-160 and SHA-1for digital signatures, and 3DES and CAST for bulk encryption of messages and files.
All versions of PGP have incorporated the routines from the freeware program ZIP (which uses routines that are comparable to the routines used in PKZip) to compress data before encryption. This is done to add security to the cryptographic implementation, as well as minimize the transmission time of the encrypted data. E-mail compatibility is achieved by Radix-64 conversion of the binary data.
PGP is bound by Federal export laws due to its usage of the RSA, IDEA, Diffie-Hellman, 3DES and CAST algorithms. The source code to PGP was legally exported in book form, and is available (along with binary distributions of the program for use outside of the USA) at http://www.pgpi.com

Define the four (4) types of PGP certificates

CISSP Seminar:

- Make up yourself
- Provided commercially
- Vouching on business relationship
- Authenticated individual activity

RSA Crypto FAQ:

Compare and contrast El Gamal and Diffie-Hellman Algorithms

CISSP Seminar:

- El Gamal
- Unpatented, public-key algorithm used for both digital signatures and encryption
- Security stems from difficulty in calculating discrete logarithms in a finite field
- First public-key crypto algorithm suitable for encryption and digital signatures unencumbered by patents in U.S.
- Diffie-Hellman
- Invented in 1976 – First public key algorithm
- Security stems from difficulty in calculating discrete logarithms in a finite field

- Used for key distribution but not for message encryption/decryption
- Patent expired in 1997

Bryce Hendrix paper on Cryptography:

El Gamal

Another popular system is the El Gamal algorithm, which relies on the difficulty of discrete logarithms. The algorithm is based on the problem of exponentiation as follows: given a modulus q and some b < q, a character x can be encrypted as integer y is the condition by º x mod q. The integer y should not be easily computable, providing security through the unfeasibility of complicated discrete logarithms.

The actual El Gamal algorithm requires, for a secure system, that everyone agrees on a large prime modulus, q. A number g is chosen such that, ideally, the order of g is q-1. The user generates a private key, y, then uses that private key to generate the public key, gy; additionally public key must be congruent to 1 mod q. For El Gamal to be secure, y must be difficult to compute from gy. Suppose Alice now wishes to encrypt a message M for Bob using his public key. Since both g and gy are known to Alice, she then computes the kth power of each and sends Bob gk and Mgy^k. Since Bob knows y, he can then reconstruct M by finding the inverse of gy^k and multiplying Mgy^k by the inverse to attain M [Achter].

Comparing the El Gamal algorithm with the RSA algorithm, it is noted that both employ exponentiation, so they can be assumed to have comparable speed in encryption and decryption as well as key gener ation. RSAs security is based on factorization, which has been studied comprehensively over the past two hundred years. El Gamal, on the other hand, relies on solving by discrete logarithms, which remains fairly unstudied. By varying g and the inverse function simultaneously an attack that has a complexity lower than solving by discrete logarithms or factoring, not it can be said that El Gamal is at best no more secure than RSA and possibly much less secure [Nechvatal]. It should also be pointed out that El Gamal requires two values to be sent, the encrypted method and a message dependent large integer- For this reason, El Gamal is said to be less space efficient than RSA, although it may present better security against some attacks, especially if k is different for gk and Mgy^k [Nechvatal].

Milgo Solution:

Diffie Hellman

Diffie Hellman was the first public key algorithm ever developed. It is still extremely popular and highly recommended for key exchange. Its primary advantage over RSA, the most widely used public key algorithm, is that Diffie Hellman is a negotiated key generation while RSA is a master/slave key generation.

The public portions of Diffie Hellman are:

Modulus = m

Integer = g

Two parties, Alice and Bob, who want to negotiate a key that only they will know, perform the following:
1.Alice generates a large random number a and computes X = ga mod m
2.Bob generates a large random number b and computes Y = gb mod m
3.Alice sends X to Bob.
4.Bob computes Key 1 = Xb mod m
5.Bob sends Y to Alice.
6.Alice computes Key 2 = Ya mod m
Both Key 1 and Key 2 are equal to gab mod m. No one besides Alice and Bob is able to generate this value. Only someone who knows a or b is able to generate the key. Therefore Diffie Hellman public key is a means for two parties who have never met to be able to negotiate a key over a public channel.
The security of Diffie Hellman revolves around the choice of the public parameters m and g. Modulus m should be a prime number and (m-1)/2 should also be a prime number. Finally modulus m should be large because the security is related to finding the discrete logarithm in a finite field of size m. SafeDial uses a 1024-bit modulus, which is considered to be highly secure by most experts.

Compare and contrast Cryptographic Module Configurations

CISSP Seminar:
There is four type of modules: inline, offline, enbedded, stand-alone

- Inline
- Front end configuration
- Module capable of accepting plaintext from source
    - Performing crypto processing
    - Passing processed data directly to communications equipment
    - Without passing back to source
- May also decrypt reverse process
- Data cannot leave host without passing through module
- Comm equip in module or external to host
- Offline
- Back end configuration
- Module capable of accepting data from source
    - Performing crypto processing
    - Passing processed data back to source

- Source responsible for storage and further transmission
    - Maintaining separation between protected and unprotected data
- Ideal for local file encryption
- Comm boards may be internal to host
- Embedded
- Module physically enclosed within and interfaces with computer
- Either inline or offline
- Less expensive
- Physical security (temper protection and detection) questionable
- Standalone
- Module contained in own physical enclosure
- Outside host computer
- Either inline or offline

Identify the Activities Related to Key management

CISSP Seminar:

- Key management
- Key change
- Key disposition
- Key recovery
- Control of crypto keys

RSA Crypto FAQ:

Key management deals with the secure generation, distribution, and storage of keys. Secure methods of key management are extremely important. Once a key is randomly generated (see Question 4.1.2.2), it must remain secret to avoid unfortunate mishaps (such as impersonation). In practice, most attacks on public-key systems will probably be aimed at the key management level, rather than at the cryptographic algorithm itself.

Users must be able to securely obtain a key pair suited to their efficiency and security needs. There must be a way to look up other people's public keys and to publicize one's own public key. Users must be able to legitimately obtain others' public keys; otherwise, an intruder can either change public keys listed in a directory, or impersonate another user. Certificates are used for this purpose.

Certificates must be unforgeable. The issuance of certificates must proceed in a secure way, impervious to attack. In particular, the issuer must authenticate the identity and the public key of an individual before issuing a certificate to that individual.
If someone's private key is lost or compromised, others must be made aware of this, so they will no longer encrypt messages under the invalid public key nor accept messages signed with the invalid private key. Users must be able to store their private keys securely, so no intruder can obtain them, yet the keys must be readily accessible for legitimate use. Keys need to be valid only until a specified expiration date but the expiration date must be chosen properly and publicized in an authenticated channel.

Compare and contrast the types of key management

CISSP Seminar:

- Link encryption
- End-To-End encryption
- Key Distribution Center (KDC)
- User unique key distributed
    - Changed infrequently
- A calls B
- Calling protocol contacts KDC
- KDC generates random session key (k)
- KDC encrypts k using A’s unique key and sends it to A
- KDC encrypts k using B’s unique key and sends it to B
- A and B uses k for session

Describe the principle of key management

CISSP Seminar:

- Must be fully automated
- For key discipline and secrecy
- No key in clear outside of crypto device
- For secrecy and known plaintext attack resistance
- Choose keys randomly from entire key space
- Pattern can be exploited by attacker to reduce work

- Key encrypting keys must be separate from data keys
- Nothing appearing in clear is encrypted with key-encrypting-key
- Keep KEK invulnerable to brute force attack
- Disguise all pattern in cleartext object before encryption
- Format, language, alphabet, public code
- To resist ciphertext only attacks
- Infrequently use keys with long life
- More key is used, more likely a successful attack and greater the consequences

Describe the concept of key recovery and key recovery systems

CISSP Seminar:

- Permits recovery of lost or damaged keys without needs to store or escrow them with a third party
- Key recovery alliance of vendors formed (10/2/96)
- Developed exportable, worldwide approach to strong encryption to enable secure international commerce
- Developing modern, high-level crypto "Key recovery" solutions
- Meet business requirements
- Ease crypto import/export restrictions worldwide
- Alliance proposed requirements for ideal key recovery system (9/19/97)

RSA Crypto FAQ:

One of the barriers to the widespread use of encryption in certain contexts is the fact that when a key is somehow "lost", any data encrypted with that key becomes unusable. Key recovery is a general term encompassing the numerous ways of permitting "emergency access" to encrypted data.

One common way to perform key recovery, called key escrow, is to split a decryption key (typically a secret key or an RSA private key) into several parts and distribute these parts to escrow agents or "trustees". In an emergency situation (exactly what defines an "emergency situation" is context-dependent), these trustees can use their "shares" of the keys either to reconstruct the missing key or simply to decrypt encrypted communications directly. This method is used by Security Dynamics' RSA SecurPC product.

Another recovery method, called key encapsulation, is to encrypt data in a communication with a "session key" (which varies from communication to communication) and to encrypt that session key with a trustee's public key. The

encrypted session key is sent with the encrypted communication, and so the trustee is able to decrypt the communication when necessary. A variant of this method, in which the session key is split into several pieces, each encrypted with a different trustee's public key, is used by TIS' RecoverKey.
Key recovery can also be performed on keys other than decryption keys. For example, a user's private signing key might be recovered. From a security point of view, however, the rationale for recovering a signing key is generally less compelling than that for recovering a decryption key.

Define Digital Signature as it Pertains to Cryptography

CISSP Seminar:

- Authentication tool to verify a message origin and a sender identity
- Resolves authentication issues
- Block of data attached to message (document, file, record, etc)
- Binds message to individual whose signature can be verified
    - By receiver or third party
    - Can’t be forged
- Each user has public-private key pair.

RSA Crypto FAQ:
The digital signature of a document is a piece of information based on both the document and the signer's private key. It is typically created through the use of a hash function and a private signing function (encrypting with the signer's private key), but there are other methods. Authentication is any process through which one proves and verifies certain information. Sometimes one may want to verify the origin of a document, the identity of the sender, the time and date a document was sent and/or signed, the identity of a computer or user, and so on. A digital signature is a cryptographic means through which many of these may be verified.

Describe the Digital Signature Standard (DSS)

CISSP Seminar:

- NIST proposed in 1991
- Uses secure hash algorithm (SHA)
- Condenses message to 160 bits
- Modular arithmetic exponentiations of large numbers
- Key size 512-1024 bits

- Difficult to invert exponentiations (security)
- Equivalent to factoring (RSA)

FIPS 186:
This Standard specifies a Digital Signature Algorithm (DSA) appropriate for applications requiring a digital rather than written signature. The DSA digital signature is a pair of large numbers represented in a computer as strings of binary digits. The digital signature is computed using a set of rules (i.e., the DSA) and a set of parameters such that the identity of the signatory and integrity of the data can be verified. The DSA provides the capability to generate and verify signatures.

Define Operation of the Digital Signature Standard

CISSP Seminar:
To sign a message

- Sender computes digest of message
- Using public hash function
- Crypto signature by sender's private key
- Applied to digest creates digital signature
- Digital signature sent with message

To verify a message

- Receiver computes digest of message
- Verifying functions with sender's public key
- Applied to digest and signature received
- Verified if both digest match
- Signature decryption identifies sender

RSA Crypto FAQ:
The digital signature is computed using a set of rules (i.e., the DSA) and a set of parameters such that the identity of the signatory and integrity of the data can be verified. The DSA provides the capability to generate and verify signatures. Signature generation makes use of a private key to generate a digital signature. Signature verification makes use of a public key which corresponds to, but is not the same as, the private key. Each user possesses a private and public key pair. Public keys are assumed to be known to the public in general. Private keys are never shared. Anyone can verify the signature of a user by employing that user's public key. Signature generation can be performed only by the possessor of the user's private key.

A hash function is used in the signature generation process to obtain a condensed version of data, called a message digest. The message digest is then input to the DSA to generate the digital signature. The digital signature is sent to the intended verifier along with the signed data (often called the message). The verifier of the message and signature verifies the signature by using the sender's public key. The same hash function must also be used in the verification process. The hash function is specified in a separate standard, the Secure Hash Standard (SHS), FIPS 180. Similar procedures may be used to generate and verify signatures for stored as well as transmitted data.

Identify the benefits of the Digital Signature Standard

CISSP Seminar:

- Provides non-repudiation
- Used with electronic contracts, purchase orders, etc…
- Used to authenticate software, data, images, users, machines.
- Protect software against viruses
- Smart card with digital signature can verify user to computer

RSA Crypto FAQ:

The digital signature is computed using a set of rules (i.e., the DSA) and a set of parameters such that the identity of the signatory and integrity of the data can be verified.

Define Non-Repudiation as it pertains to Cryptography

CISSP Seminar:

- Proves message sent and received
- Ensures sender can’t deny sending
- Recipient can’t deny claim that they received something else or deny receiving proper message

Define Hash functions as they pertain to Cryptography

CISSP Seminar:

RSA Crypto FAQ:

The main role of a cryptographic hash function is in the provision of message integrity checks and digital signatures. Since hash functions are generally faster than encryption or digital signature algorithms, it is typical to compute the digital signature or integrity check to some document by applying cryptographic processing to the document's hash value, which is small compared to the

document itself. Additionally, a digest can be made public without revealing the contents of the document from which it is derived. This is important in digital timestamping where, using hash functions, one can get a document timestamped without revealing its contents to the timestamping service.

Describe the Use of Certification Authority

CISSP Seminar:

- Binds individuals to their public keys
- Certification authrority's digital signature
- Attest binding
- Certification authority certification
- User identification, public key, date
- X509 certification standard
- NIST National Digital Signature Certification Authority study

RSA Crypto FAQ:

Certificates are issued by certification authority. Certificates are digital documents attesting to the binding of a public key to an individual or other entity. They allow verification of the claim that a specific public key does in fact belong to a specific individual. Certificates help prevent someone from using a phony key to impersonate someone else. In some cases it may be necessary to create a chain of certificates, each one certifying the previous one until the parties involved are confident in the identity in question.

In their simplest form, certificates contain a public key and a name. As commonly used, a certificate also contains an expiration date, the name of the certifying authority that issued the certificate, a serial number, and perhaps other information. Most importantly, it contains the digital signature of the certificate issuer. The most widely accepted format for certificates is defined by the ITU-T X.509 international standard; thus, certificates
can be read or written by any application complying with X.509.

Define Electronic Document Authorization (EDA)

CISSP Seminar:

- Authorizes certificates
- Specifies public key holder authority/power
- Spend, authorize payments, perform business functions
- Specifies limits to prevent abuse
- Cosignature requirements

- Enalbles checks and balances

Define and distinguish between message authentication code and Code Generation

CISSP Seminar:

Message Authentication:

- Simple MACing
- Weakest form of authentication
- MAC generation standard – ANSI X9.9 (FIMAS)
- Computed value derived from document
- Detect accidental/intentional alteration
- Forgery possible

MAC Generation

- Algorithm examines bitstream
- Data field output appended to bitstream
- Before transmission/storage
- Parity/checksum application
- Bitstream and MAC
- Machine/communications error

RSA Crypto FAQ:

A message authentication code (MAC) is an authentication tag (also called a checksum) derived by appying an authentication scheme, together with a secret key, to a message. Unlike digital signatures, MACs are computed and verified with the same key, so that they can only be verified by the intended recipient. There are four types of MACs: (1) unconditionally secure, (2) hash function-based, (3) stream cipher-based, or (4) block cipher-based.

Simmons and Stinson [Sti95] proposed an unconditionally secure MAC based on encryption with a one-time pad. The ciphertext of the message authenticates itself, as nobody else has access to the one-time pad. However, there has to be some redundancy in the message. An unconditionally secure MAC can also be obtained by use of a one-time secret key.

Hash function-based MACs (often called HMACs) use a key or keys in conjunction with a hash function to produce a checksum that is appended to the message. An example is the keyed-MD5 method of message authentication.

Describe Bitstream Authentication

CISSP Seminar:

- Generate new MAC
- Compare with original
- Mac Algorithm qualities
- Sensitive to bit changes
- Creates MAC unable to be duplicated

Describe brute force attack as they pertain to Cryptography

CISSP Seminar:
Trying all keys
RSA Crypto FAQ:
Exhaustive key search, or brute-force search, is the basic technique of trying every possible key in turn until the correct key is identified. To identify the correct key it may be necessary to possess a plaintext and its corresponding ciphertext, or if the plaintext has some recognizable characteristic, ciphertext alone might suffice. Exhaustive key search can be mounted on any cipher and sometimes a weakness in the key schedule of the cipher can help improve the efficiency of an exhaustive key search attack.
Advances in technology and computing performance will always make exhaustive key search an increasingly practical attack against keys of a fixed length. When DES was designed, it was generally considered secure against exhaustive key search without a vast financial investment in hardware. To date, there is no public evidence that such hardware has been constructed. Over the years, however, this line of attack will become another increasingly attractive to a potential adversary useful article on exhaustive key search can be found in the Winter 1997 issue of CryptoBytes available online at the following URL:
http://www.rsa.com/rsalabs/pubs/cryptobytes/html/article_index.html

Compare and contrast the cost and time taken in Brute Force Attacks

CISSP Seminar:
Cost of brute force:
Year MIPs Year Cost 56 bit key 40 Bit key
1997 $15.00 $17.0M $260.00
2002 $1.50 $1.7M $26.00
2007 $0.15 $170,000 $2.60
Time for brute force:
Key tested per second 56 bit key 40 bit key
1,000 300,000,000 years 17.5 years
1,000,000 300,000 years 6.2 days
1,000,000,000 300 years 9.0 minutes
1,000,000,000,000 109 days .5 seconds

RSA Crypto FAQ:

While exhaustive search of DES's 56-bit key space would take hundreds of years on the fastest general purpose computer available today, the growth of the Internet has made it possible to utilize thousands of such machines in a distributed search by partitioning the key space and distributing small portions to each of a large number of computers. In January 1999, the DES Challenge III was solved in just 22 hours and 15 minutes by the Electronic Frontier Foundation´s `Deep Crack´ in a combined effort with distributed.net.
While the 56-bit key in DES now only offers a few hours of protection against exhaustive search by a modern dedicated machine [Wie94], the current rate of increase in computing power is such that an 80-bit key as used by Skipjack can be expected to offer the same level of protection against exhaustive key search in 18 years time as DES does today [BDK93]. Absent a major breakthrough in quantum computing, it is unlikely that 128-bit keys, such as those used in IDEA or RC5-32/12/16, will be broken by exhaustive search in the foreseeable future.

Compare and contrast Brute Force, Analytic, Statistical, and Implementation Attacks

CISSP Seminar:

- Analytic
- Using algorithm and algebraic manipulation weakness to reduce complexity
- RSA factoring attack
- Double DES attack
- Statistical
- Using statistical weakness in design
- More 1’s than 0’s in the keystream
- Implementation
- Using the specific implementation of the encryption protocol
- 95 attack of netscape key
    - deficient key randomization
    - string algorithm + 128 bit key

Describe the Commercial COMSEC Endorsement Program (CCEP)

CISSP Seminar:
Commercial communications security endorsement program

- NSA and industry relationship

- Combine government crypto knowledge with industry product-development expertise
- Type 1 or type 2 high-grade crypto products.
- Type 1 encrypt classified and SUI
    - STU Secure telephone unit
- Type 2 encrypts SUI
    - Authentication devices, transmission security devices, secure LAN's

The journal of American Undergroung Computing:
In the mid-80's, NSA introduced a program called the Commercial COMSEC Endorsement Program, or CCEP.
CCEP was essentially Clipper in a black box, since the technology was not sufficiently advanced to build lower-cost chips. Vendors would join CCEP (with the proper security clearances) and be authorized to incorporate classified algorithms into communications systems. NSA had proposed that they themselves would actually provide the keys to end-users of such systems.

Define the levels of Encryption as Defined in the CCEP

CISSP Seminar:

- Type 1 or type 2 high-grade crypto products.
- Type 1 encrypt classified and SUI
    - STU Secure telephone unit
- Type 2 encrypts SUI
    - Authentication devices, transmission security devices, secure LAN's

Compare and contrast the differences in Export Issues regarding Encryption

CISSP Seminar:
This has to be completed.
RSA Crypto FAQ:
Cryptography is export-controlled for several reasons. Strong cryptography can be used for criminal purposes or even as a weapon of war. During wartime, the ability to intercept and decipher enemy communications is crucial. For that reason, strong cryptography is usually classified on the U.S. Munitions List as an export-controlled commodity, just like tanks and missiles.
Cryptography is just one of many technologies which is covered by the ITAR (International Traffic in Arms Regulations).
In the United States, government agencies consider strong encryption to be systems that use RSA with key sizes over 512-bits or symmetric algorithms (like

DES, IDEA, or RC5) with key sizes over 40-bits. Since government encryption policy is heavily influenced by the agencies responsible for gathering domestic and international intelligence (the FBI and NSA, respectively) the government is compelled to balance the conflicting requirements of making strong cryptography available for commercial purposes while still making it possible for those agencies to break those codes, if need be. The US government does, however, allow 56-bit block ciphers to be exported for financial cryptography.