CES - Introduction to Cryptography (C839)
Video Notes
Learning Resource Page 1.2
Episode Title: History of Cryptography

Cryptography is the study of secure communication mechanisms / methods. It provides ways to encode a message so that it cannot be read by outsiders.

Mono-Alphabet Substitution Ciphers: (Single Alphabet)
Atbash - Reverses the alphabet (A becomes Z, B becomes Y ...)
Ceasar - Choose some number by which to shift each letter of the message. (right is "+" | left is "-" | A "+2" = C | C "-1" = B)
ROT-13 - Rotate all characters 13 letters through the alphabet (A becomes N, B becomes O ...)
Scytale - Use of a rod of a certain length to create/encrypt a message, and same rod must be used
to read/decrypt the message by the recipient
All single-alphabet substitution ciphers preserve the underlying letter and word frequency and are vulnerable to cryptanalysis as a result.
Multi-Alphabet Substitution Ciphers add complexity by adding alphabets to be used for the substitution rounds.
Example: We are using three alphabets to do the shifting, each represented by a "+" or a "-" value. When we run out of alphabets, we start over again with the first one, effectively "roundrobining"
through the text until it is all shifted.
A DOG (+1-2+1)
B BPH
The cipher disk: a physical device used to encrypt. Invented by Leon Alberti in 1466. The cipher disk was polyalphabetic; each time you turned the disk, you used a new cipher.
The Vigenère cipher: invented in 1553 by Giovan Battista Bellaso, but is named for Blaise de Vigenère who developed a stronger version of the cipher. It is a method of encrypting by using a series of interwoven Caesar ciphers based on the letters of a keyword. It is considered a polyalphabetic cipher system. Friedrich Kasiski published the first successful attack against the Vigenère cipher in 1863.
The Playfair Cipher: invented by Charles Wheatstone in 1854. Uses a five-by-five table containing a keyword or key phrase. To generate the key table, one would first fill in the spaces in the table with the letters of the keyword (dropping any duplicate letters), then fill in the remaining spaces with the rest of the letters of the alphabet in order. The technique encrypts pairs
of letters (digraphs), instead of single letters as in the simple substitution cipher. The Playfair is significantly harder to break since the frequency analysis used for simple substitution ciphers does not work with it. A typical 5x5 key square is below: (Any sequence of 25 letters can be used as a key, so long as all letters are in it and there are no repeats. Note that there is no 'j', it is

combined with 'i'.)
k e y w o
r d a b c
f g h i l
m n p q s
t u v w x

The ADFGVX Cipher: the first cipher used by the German Army during World War I. Invented by Colonel Fritz Nebel in 1918. A transposition cipher which used a modified Polybius square with a single columnar transposition used to encode a 36 letter alphabet. The key for this algorithm is a six-by-six square made up of the letters ADFGVX forming the outer row and column, the rest of the table is comprised of the letters of the alphabet and the numbers 0 through
9 distributed randomly in the square. Example is below: (you encrypt message by finding it's coordinates on the grid and using the row and column coordinates as the encrypted representation of the plaintext - each plaintext character becomes two encrypted characters in other words)
A D F G V X
A 1 Q 2 E T P
D W R U I 9 O
F Y 3 4 A S F
G 5 H 6 J L K
V G D 7 Z 0 X
X C V B N M 8
Plaintext = DOG
Ciphertext = DVXDAV
The ENIGMA Machine: a multi-alphabet substitution cipher using machinery to accomplish the encryption. In World War II, the Germans used this as an electromechanical rotor-based cipher system.
Demo Cryptool: https://www.cryptool.org/en/cryptool2
Learning Resource Pages 2.1, 2.3, 3.5, and 4.2
This video is divided into several parts and can be found on multiple pages.

Episode Title: Symmetric Cryptography and Hashes
Symmetric encryption is expressed mathematically as:
C = E(k,p)
Cipher text (C) is equal to the encryption function (E) with the key (k) and plaintext (p) being passed as parameters to that function.
Symmetric decryption is expressed mathematically as:
P = E(k,c)
Important concepts from Information Theory published in 1949 by Claude Shannon in the Bell System Technical Journal:
1. Diffusion
2. Confusion
3. Avalanche effect - Horst Feistel's variation on Shannon's concept of diffusion
Kerckhoffs's Principle: In 1883, Auguste Kerckhoff proposes that a cryptosystem should be secure even if all of the elements of the system, except the key, is public knowledge.

A deeper dive into the **Feistel Network**:
Starts by splitting the block of plaintext data into two parts (termed L0 and R0). Usually the split is equal, but not always, as the Unbalanced Feistel Cipher uses a split that is unequal.
The "round function" F is applied to one of the halves. The term round function refers to a function performed with each iteration of the Feistel cipher. (The details of the round function F can vary with different implementations.)
The output of each round function F is then XORed with the other half.
For example, take L0, pass it through the round function F, then take the result and XOR it with R0. Then the halves are transposed. So L0 gets moved to the right and R0 gets moved to the left.
This process is repeated a given number of times.
The main difference between cryptography algorithms is the exact nature of the round function F, and the number of iterations.

Data Encryption Standard (DES): 64-bit algorithm, operating at 56-bits due to 8-bit parity block being used
The basic operation of DES is:
1. Data is divided into 64-bit blocks.
2. That data is then manipulated by 16 separate steps of encryption involving substitutions, bit-shifting, and logical operations using a 56-bit key.
3. Data is then further scrambled using a swapping algorithm.
4. Data is finally transposed one last time.
DES uses eight "S-boxes" (Substitution Boxes), which are basically look up tables. Each S-box has a table that determines, based on the bits passed into it, what to substitute for those bits. Each
item passed into the box is substituted with the item that matches it in the lookup table. Each one
of the DES S-boxes takes in 6 bits and produces 4 bits. The middle 4 bits of the 6-bit input are

used to look up the 4-bit replacement bits.
3DES (Triple DES)
3DES uses a “key bundle” which comprises three DES keys, K1, K2, and K3. Each key is standard 56-bit DES key. It will then apply the following process:
DES encrypts with K1, decrypts with K2, then encrypts again with K3.

DESx
This is a variation of DES that XORs another 64-bit key to the plaintext before applying the DES algorithm. The concept of simply XORing in an additional key is called whitening. This adds to the confusion of the resultant text.

Advanced Encryption Standard (AES) | Rijndael - replacement for DES as of 2001 - formally announced by NIST as FIPS 197.
AES can have three different key sizes. They are: 128, 192, or 256 bits. The three different implementations of AES are referred to as AES 128, AES 192, and AES 256. All three operate on a block size of 128 bits.
AES uses a substitution-permutation matrix rather than a Feistel network. AES operates on a four-by-four column major order matrix of bytes, called the state.
AES general steps are:
1. **Key expansion:** Round keys are derived from the cipher key using Rijndael's key schedule.
2. **Initial round:**
a. AddRoundKey - Each byte of the state is combined with the round key using bitwise XOR.
3. **Rounds:**
SubBytes - A non-linear substitution step where each byte is replaced with another according to a lookup table. (lookup table is called a Rijndael S-Box)
ShiftRows - A transposition step where each row of the state is shifted cyclically a certain number of steps.
MixColumns - A mixing operation which operates on the columns of the state, combining the four bytes in each column.
AddRoundKey
4. **Final round** (no MixColumns used):
SubBytes
ShiftRows
AddRoundKey
Blowfish: A 16-round Feistel cipher working on 64-bit blocks. Unlike DES, it can have varying key sizes ranging from 32 bits to 448 bits. Designed by Bruce Schneier.
Serpent: Like AES, Serpent has a block size of 128 bits and can have a key size of 128, 192, or 256 bits. The algorithm is also a substitution-permutation network like AES. It uses 32 rounds working with a block of four 32-bit words. Each round applies one of eight 4-bit to 4-bit S-boxes 32 times in parallel. Designed by Ross Anderson, Eli Biham, and Lars Knudsen.
Twofish: Uses a block size of 128 bits and key sizes up to 256 bits. It is a Feistel cipher.

Designed by Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson.
Skipjack: Developed by the NSA for use in the clipper chip. Skipjack uses an 80-bit key to encrypt or decrypt 64-bit data blocks. It is an unbalanced Feistel network with 32 rounds.
IDEA (International Data Encryption Algorithm): Designed by James Massey and Xuejia Lai. Operates on 64-bit blocks and has a 128-bit key. The algorithm consists of a series of eight identical transformations for each round, and an output transformation.
Stream Ciphers
RC4
FISH
PIKE
RC4: The algorithm is used identically for encryption and decryption as the data stream is simply XORed with the key. RC4 uses a variable length key from 1 to 2048 bits, (minimum of 40 bits or higher to be considered secure). That key constitutes a state table that is used for subsequent generation of pseudo-random bytes and then to generate a pseudo-random stream which is XORed with the plaintext to produce the ciphertext.
FISH (Fibonacci Shrinking): Published by Siemens in 1993. A software-based stream cipher using a Lagged Fibonacci generator (pseudorandom number generator).
PIKE: Improvement on FISH due to vulnerability to known-plaintext attacks. Published by Ross Anderson.
Hash function: a one-way mathematical operation that reduces a message or data file into a smaller fixed length output, or hash value
Variable data input (of any size) + hashing algorithm = fixed bit stream output (hash value)
MD5 = 128 bits
SHA1 = 160 bits
"Salting the Hash"
Refers to random bits that are used as one of the inputs to the hash. The salt is intermixed with the message that is to be hashed. Very effective against rainbow table attacks. The salt value should be kept secret in order to maximize its positive impact on the security of the secret data.
Additional Hashing Algorithms:
FORK-256
RIPEMD-160 (RACE Integrity Primitives Evaluation Message Digest): developed by Hans Dobbertin, Antoon Bosselaers, and Bart Preneel. The size of a RIPEMD-160 hash value is 160 bits.
GOST: initially defined in the Russian national standard GOST R 34.11-94 "Information Technology - Cryptographic Information Security - Hash Function". The size of a GOST hash value is 256 bits.
TIGER: designed by Ross Anderson and Eli Biham in 1995. The size of a Tiger hash value is 192 bits.
http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf
Binary Math Table
decimal
(base 10)

binary
(base 2)
expansion
0 0 0 ones
1 1 1 one
2 10 1 two and zero ones
3 11 1 two and 1 one
4 100 1 four, 0 twos, and 0 ones
5 101 1 four, 0 twos, and 1 one
6 110 1 four, 1 two, and 0 ones
7 111 1 four, 1 two, and 1 one
8 1000 1 eight, 1 four, 0 twos, and 0 ones
9 1001 1 eight, 0 fours, 0 twos, and 1 ones
10 1010 1 eight, 0 fours, 1 two, and 0 ones
11 1011 1 eight, 0 fours, 1 two, and 1 one
12 1100 1 eight, 1 four, 0 twos, and 0 ones
13 1101 1 eight, 1 four, 0 twos, and 1 one
14 1110 1 eight, 1 four, 1 two, and 0 ones
15 1111 1 eight, 1 four, 1 two, and 1 one
16 10000 1 sixteen, 0 eights, 0 fours, 0 twos, and 0
ones
Operations:
1. AND
2. OR
3. XOR - (Exclusive OR)
Binary AND - If both numbers have a one in both places, then the resultant number is a one. If not, then the resultant number is a zero.
1st - 1100
2nd - 0100
==========
Result - 0100
Binary OR - Checks to see whether there is a one in either or both numbers in a given place. If so, then the resultant number is one. If not, the resultant number is zero.
1st - 1010
2nd - 0100
==========
Result - 1110
Binary XOR (Exclusive OR) - The binary XOR operation (also known as the binary XOR function) will always produce a 1 output if either of its inputs is 1 and will produce a 0 output if both of its inputs are 0 or 1.
1st - 1110
2nd - 0101
==========

Result - 1011
XORing is reversible. If you XOR the resultant number with the second number, you get back the first number. Conversely, If you XOR the resultant number with the first number, you get the
second number.
Symmetric key cryptography uses two processes: Substitution and Transposition.
The substitution portion is accomplished by XORing the plaintext message with the key. The transposition is done by swapping blocks of the text.
A key schedule is also used by many Symmetric algorithms. It is an algorithm that, given the key, calculates the subkeys for these rounds.
Two types of Symmetric Algorithms:
1. Block
2. Stream

Block Algorithm Examples:
The Feistel Network - (Feistel Function | Feistel Cipher)
Block Algorithm Examples Cont.
DES
3DES (Triple DES)
DESX
AES see link http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf
Blowfish
Serpent
Twofish
Skipjack
IDEA

Learning Resource Pages 2.3 and 2.5
This video is divided into several parts and can be found on two pages.
Episode Title: Crypto Definitions
Key clustering: different encryption keys generate the same ciphertext from the same plaintext message
Synchronous: encryption or decryption request is performed immediately
Asynchronous: Encrypt/Decrypt requests are processed in queues
Hash function: a one-way mathematical operation that reduces a message or data file into a smaller fixed length output, or hash value
● Variable data input (of any size) + hashing algorithm = fixed bit stream output (hash value)
○ MD5 = 128 bits
○ SHA1 = 160 bits
Digital signatures: provide authentication of a sender and integrity of a sender's message. A message is input into a hash function. Then the hash value is encrypted using the private key of the sender. The result of these two steps yields a digital signature
Symmetric: A single key used to encrypt and to decrypt
Asymmetric: two different but mathematically related keys are used where one key is used to encrypt and another is used to decrypt
Digital certificate: used to identify the certificate holder when conducting electronic transactions
– Type of certificates currently used = X.509 v3
Certificate authority (CA): an entity trusted by one or more users as an authority in a network that issues, revokes, and manages digital certificates
● Root CA – only issues certificates to Subordinate CA's
● Subordinate CA – issues certificates to users + computers on behalf of the Root CA
Registration authority (RA): responsible for the accuracy of the information contained in a certificate request. The RA is also expected to perform user validation before issuing a certificate
request
Plaintext or cleartext
Ciphertext or cryptogram
Cryptosystem: This represents the entire cryptographic operation. This includes the algorithm, key, and key management functions
Encryption
Decryption
Key or Cryptovariable: The input that controls the operation of the cryptographic algorithm
Non-repudiation
Algorithm
Cryptanalysis: study of techniques for attempting to defeat cryptographic techniques and information security services
Cryptology: the science that deals with hidden, disguised, or encrypted communications
Collision: occurs when a hash function generates the same output for different inputs

Key space: represents the total number of possible values of keys in a cryptographic algorithm or
other security measure, such as a password
Work factor: the time and effort required to break a protective measure
Initialization vector (IV): A non-secret binary vector used as the initializing input algorithm for the encryption of a plaintext block sequence to increase security by introducing additional cryptographic variance
Encoding: The action of changing a message into another format through the use of a code
Decoding: The reverse process from encoding – converting the encoded message back into its plaintext format
Transposition or permutation
Substitution
SP-network: substitution and permutation (transposition), most block ciphers do a series of repeated substitutions and permutations to add confusion and diffusion to the encryption process
Confusion: provided by mixing (changing) the key values used during the repeated rounds of encryption
Diffusion: provided by mixing up the location of the plaintext throughout the ciphertext
Avalanche effect: where a minor change in either the key or the plaintext will have a significant change in the resulting ciphertext
Stream Cipher
Block Cipher
Electronic Code Book (ECB) – Each block is encrypted independently, BUT identical plaintext blocks are encrypted into identical ciphertext blocks
Cipher Block Chaining (CBC) – Each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block depends on all plaintext blocks processed up to that point. To make each message unique, an initialization vector must be used in
the first block.
Propagating Cipher Block Chaining (PCBC) – Each block of plaintext is XORed with the XOR of the previous plaintext block and the previous ciphertext block before being encrypted. As with
CBC mode, an initialization vector is used in the first block.
Cipher Feedback (CFB): Allows encryption of partial blocks rather than requiring full blocks for encryption. This eliminates the need to pad a block like in CBC.
The Output Feedback (OFB) mode makes a block cipher into a synchronous stream cipher. It generates keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext.
● Like OFB, Counter mode turns a block cipher into a stream cipher. It generates the next keystream block by encrypting successive values of a "counter".
Symmetric Cryptography: "Single Key" (private key) is used to both encrypt and decrypt. Show diagram to explain private key.
Learning Resource Pages 2.3, 9.3

This video is divided into several parts and can be found on two pages.
Episode Title: Asymmetric Cryptography
Asymmetric Cryptography: "Public / Private Key Pair" one key is used to encrypt and the other to decrypt.
Diffusion: Having changes to one character in the plaintext affect multiple characters in the ciphertext.
Confusion: Making the relationship between the statistical frequencies of the ciphertext and the
actual key as complex as possible. This occurs by using a complex substitution algorithm.
Avalanche: A small change yields large effects in the output. This is Feistel's varaiation on Shannon's concept of Diffusion. Ideally, a change in one bit in the plaintext would affect all the bits of the ciphertext. This would be a complete avalanche.
In information theory, entropy is a measure of the uncertainty associated with a random variable.
Shannon's source coding theorem: it is impossible to compress the data such that the code rate is
less than the Shannon entropy of the source, without it being virtually certain that information will be lost.
Number Groupings:
N = Natural Numbers (1,2,3,4,etc..)
Z = Integers (Natural numbers + 0 + negative numbers | any number that can be written without a fractional component)
Q = Rational numbers (numbers expressed as the ratio of integers, or fractions)
R = Real numbers (include all the rational numbers, such as the integer ,àí3 and the fraction 5/4, and all the irrational numbers, such as ,àö2)
i = Imaginary numbers (numbers whose square is a negative)
Prime Numbers: any number whose factors are 1 and itself
Co-Prime Numbers: a number that has no factors in common with another number (3 & 7)
Eulers Totient: counts the positive integers up to a given integer n that are relatively prime to n. For example, 7 has six numbers that are co-prime to it.
Modulus Operator: divide A by N and return the remainder. (sometimes symbolized as %, as in 9 % 2= 1)
5 mod 2 = 1
12 mod 5 = 2
Fibonacci Numbers: Sequence of numbers derived by adding the last number in the sequence to
the previous one to create the next
Example: 1,1,2,3,5,8,13,21,35,56,91
Birthday Problem/Paradox - "How likely it is that any two people in a room of 23 would have the same birthday?"
- (22+21+20+19+18+17+16+15+14+13+12+11+10+9+8+7+6+5+4+3+2+1 = 253) - total number of possible combinations among a group of 23 people
- The probability reaches 100% when the number of people reaches 367 (since there are

only 366 possible birthdays, including February 29). 99.9% probability is reached with just 70 people, and 50% probability with 23 people.
Birthday Attack - A birthday attack is a name used to refer to a class of brute force attacks based
on the birthday paradox.
● If you have an encryption algorithm with a key space of 32 bits, you can generate 4,294,967,295 random keys, (65,535 keys) and have a 50% chance of finding the right key. For a guaranteed match, you would have to generate 4,294,967,295 random keys. The birthday paradox means that one can try a set of random keys that is much smaller than the entire key space, and have a good chance of getting a match.
Pseudo-random number generators (PRNGs) are algorithms that can create long runs of numbers with good random properties, but eventually the sequence repeats.
The German Federal Office for Information Security (BSI) has established four criteria for quality of random number generators:
● K1: A sequence of random numbers with a low probability of containing identical consecutive elements.
● K2: A sequence of numbers which is indistinguishable from "true random" numbers according to specified statistical tests.
● K3: It should be impossible for any attacker to calculate, or otherwise guess, from any given subsequence, any previous or future values in the sequence.
● K4: It should be impossible for an attacker to calculate, or guess from an inner state of the generator, any previous numbers in the sequence or any previous inner generator states.
To be suitable for cryptography, any PRNG should meet K3 and K4 standards.
Examples of PRNGs:
● Naor-Reingold
● Mersenne Twister
● Linear Congruential Generator
● Lehmer Random Number Generator (twisted generalized feedback shift registers)
● Lagged Fibonacci Generator (LFG) - If addition is used, then it is an Additive Lagged Fibonacci Generator or ALFG. If multiplication is used, it is a Multiplicative Lagged Fibonacci Generator or MLFG. If the XOR operation is used, it is called a two-tap generalized feedback shift register, or GFS.
Diffie-Hellman: (The first publicly described asymmetric algorithm)
A cryptographic protocol that allows two parties to establish a shared key over an insecure channel. Often used to allow parties to exchange a symmetric key through some unsecure medium, such as the Internet. It was developed by Whitfield Diffie and Martin Hellman in 1976.
RSA: developed in 1977 by three mathematicians, Ron Rivest, Adi Shamir, and Len Adleman. Based on the practical difficulty of factoring the product of two large prime numbers. Key sizes are typically from 1,024 - 4,096 bits.
Menezes-Qu-Vanstone (MQV): A protocol used for key agreement that is based on Diffie-Hellman. It is incorporated in the public key standard IEEE P1363.
Digital Signature Algorithm (DSA): described in U.S. Patent 5,231,668, filed July 26, 1991, and

attributed to David W. Kravitz. It was adopted by the U.S. government in 1993 with FIPS 186.
Elliptic Curve Cryptography (ECC): The security of Elliptic Curve cryptography is based on the fact that finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is difficult to the point of being impractical to do so.
- Elliptic Curve Diffie Hellman (used for key exchange)
- Elliptic Curve Digital Signature Algorithm (ECDSA)
- Elliptic Curve MQV key agreement protocol

ElGamal: Based on Diffie-Hellman and was invented in 1984 by Taher Elgamal. It is used in some PGP implementations as well as GNU Privacy Guard software. The algorithm consists of three parts: the key generator, the encryption algorithm, and the decryption algorithm.
Learning Resource Pages 7.6, 17.2, 19.1, 19.6, 24.1
This video is divided into several parts and can be found on multiple pages.

Episode Title: Applications of Cryptography

Digital Certificates: A certificate is a digital representation of information that identifies you as a relevant entity

Most widely deployed/issued certificate template/type in the world is (X.509v3), first used in July of 1988.

The content of an X.509 certificate includes the following:

- Version
- Certificate holder's public key
- Serial number
- Certificate holder's distinguished name
- Certificate's validity period
- Unique name of certificate issuer
- Digital signature of issuer
- Signature algorithm identifier

Public Key Infrastructure (PKI)

Certificate Authority (CA): primary role of the CA is to digitally sign and publish the public key bound to a given user. It is an entity trusted by one or more users to manage certificates.

Registration Authority (RA): acts as a proxy between the user and the CA. The RA receives a certificate request, authenticates it, and forwards it to the CA.

Certificate Revocation List (CRL): a list of certificates that have been revoked. CAs publish their own CRLs.

Online Certificate Status Protocol (OCSP): a real-time protocol for verifying certificates.

Server-based Certificate Validation Protocol (SCVP): RFC 5055. An Internet protocol for determining the path between a X.509 digital certificate and a trusted root (Delegated Path Discovery) and the validation of that path (Delegated Path Validation) according to a particular validation policy.

Certificate Classes:

Class 1 - for individuals, intended for email

Class 2 - for organizations for which proof of identity is required

Class 3 - for servers and software signing, for which independent verification and checking of identity and authority is done by the issuing CA

Class 4 - for online business transactions between companies

Class 5 - for private organizations or governmental security

Certificate Management (Certificate Lifecycle)

Setup and Initialization Phase

Registration

Key Pair Generation

Certificate Generation

Certificate Dissemination

Administration Phase

Key storage

Certificate retrieval and validation

Backup or escrow

Recovery
Cancellation and History Phase
Expiration
Renewal
Revocation
Suspension
Destruction
Update and Patch Vulnerabilities
Person who can recover keys from the keystore on behalf of a user
Issue recovery agent certificate
EFS Recovery Agent certificate
Key Recovery Agent certificate
Trust Models:
Single Authority
Hierarchical
Web of Trust
Authentication Protocols:
Password Authentication Protocol (PAP) - transmission of user name and password in the clear. Basic HTTP Authentication uses PAP.
Shiva Password Authentication Protocol (S-PAP) - extends PAP by encrypting username and password transmission.
Challenge Handshake Authentication Protocol (CHAP) - calculates a hash after the user has logged in, then it shares that hash with the client system. Periodically, the server will ask the client to provide that hash (this is the challenge part). If the client cannot, then it is clear that the
communications have been compromised. MS-CHAP is a Microsoft-specific extension to CHAP.
Kerberos: A user logs in, the authentication server verifies their identity and then contacts the ticket granting server (these are often on the same machine). The ticket granting server sends an
encrypted ticket to the uses machine. When the user needs to access some resource on the network the user's machine uses that ticket granting ticket to gain access to the target machine.
Kerberos Components:
1. **Principal:** Any server or client that can be assigned a ticket.
2. **Authentication Server (AS):** Server that authorizes the principal and connects them to the ticket granting server.
3. T**icket Granting Server (TGS):** Issues tickets.
4. **Key Distribution Center (KDC):** Server that provides the initial ticket and handles TGS requests.
5. **Realm:** A boundary within an organization. Each realm has its own AS and TGS.
6. **Ticket Granting Ticket (TGT):** Ticket that is granted during the authentication process.
7. **Ticket:** Used to authenticate. Contains the identity of the client, the session key, the

timestamp, and the checksum. Encrypted with the servers key.
8. **Session Key:** Temporary encryption key.
The Kerberos process:
1. User sends credentials to the AS that will authenticate them.
2. The AS authenticates the user and issues a TGT.
3. The user's computer presents the TGT to the TGS when the user wants to access a network resource. The TGS will use the AS to authenticate that ticket. If it is authentic, then a specific resource ticket and a session key are issued and sent to the user's computer.
4. The user presents that ticket/key to the resource.
5. The resource verifies that ticket with the TGS.
6. Then the user is authorized to access the resource.
Pretty Good Privacy (PGP): created by Phillip Zimmerman. It is an application that is designed to make encryption/decryption accessible to anyone that wants to use it.
A PGP certificate includes the following:
PGP version number
Certificate holder's public key
Certificate holder's information
Digital signature of certificate owner
Certificate validity period
Preferred symmetric encryption algorithm for the key
Wifi Encryption:
• Wired Equivalent Privacy (WEP) - uses the stream cipher RC4 to secure the data and a CRC-32 checksum for error checking. Standard WEP uses a 40-bit key with a 24-bit initialization vector (IV).
• WiFi Protected Access (WPA) - Replaces RC4 with Temporal Key Integrity Protocol (TKIP), which is a 128-bit per-packet key, meaning that it dynamically generates a new key for each packet.
• WPA-2 - Based on the IEEE 802.11i standard. Uses AES with CCMP to provide for enhanced confidentiality, integrity and authentication.
• WPA-2 Enterprise - Also referred to as WPA-802.1x mode. Requires a RADIUS authentication server. An Extensible Authentication Protocol (EAP) is used for authentication.
Secure Socket Layer (SSL)/ Transport Layer Security (TLS):
How SSL works:
1. The browser asks the web server to prove its identity.
2. The server sends back a copy of its SSL certificate.
3. The browser checks to see if the certificate is from a CA it trusts.
4. The server sends back a digitally signed acknowledgement and a session is started.
How TLS works:
A TLS client and server negotiate a connection by using a handshaking procedure. The handshake begins when a client connects to a TLS-enabled server requesting a secure connection

and presents a list of encryption and hash functions it can support. From this list, the server picks
the strongest encryption and hash function that it also supports and notifies the client of the chosen algorithms. The server sends back its identification in the form of a digital certificate. This is a standard X.509 certificate. (The client may contact the CA that issued the certificate and
confirm the validity of the certificate before proceeding.) In order to generate the session keys used for the secure connection, the client encrypts a random number with the server's public key
and sends the result to the server. The server decrypts that number with its private key. From the
random number, both parties generate key material for encryption and decryption.
Virtual Private Network (VPN) - Used to extend access to a private network over a public network such as the Internet.
Protocols that are often used to create VPNs:
Point to Point Tunneling Protocol (PPTP): Works at Layer 2 of the OSI model. Offers the ability to encrypt and authenticate. Uses Extensible Authentication Protocol (EAP) and/or Challenge Handshake **Authentication Protocol (CHAP)** to authenticate. Uses **Microsoft Point to Point Encryption (MPPE)** for encryption. (MPPE is a derived version of DES). PPTP ONLY works over standard IP Networks.
Layer 2 Tunneling Protocol (L2TP): Works at Layer 2 of the OSI model. Combination of PPTP and Cisco's Layer 2 Forwarding Protocol (L2F). Offers additional methods for authentication; PPTP offers two, whereas L2TP offers five. In addition to CHAP and EAP, L2TP offers PAP, SPAP, and MS-CHAP. L2TP works over standard IP networks, but also X.25 and ATM.
Internet Protocol Security (IPSec): Used with L2TP VPN's to provide the encryption capability required to protect data.
SSL/TLS VPN: Used to establish a VPN via a web browser.
Encrypting File System (EFS)
EFS is a Microsoft technology that lets you encrypt data on your computer, and control who can decrypt, or recover, the data. To use EFS, all users must have EFS certificates. EFS users must also have NTFS permission to modify the files. Users need to backup their EFS key in order to ensure that it will be available if required to be used.
How to backup an EFS key:
1. Open a Command Prompt.
2. Insert the removable media that you're using to store your certificate.
3. Navigate to the directory on the removable media drive where you want to store the recovery certificate by typing drive letter, and then press "Enter".
4. Type "cipher /r:file name" , and then press "Enter". If you're prompted for an administrator password or confirmation, type the password or provide confirmation.
How to restore an EFS key:
1. Insert the removable media that contains your recovery certificate.
2. Click the Start button. In the search box, type "secpol.msc", and then press "Enter". (If you're prompted for an administrator password or confirmation, type the password or

provide confirmation.)
3. In the left pane, select "Public Key Policies", right-click "Encrypting File System", and then click "Add Data Recovery Agent". This opens the Add Recovery Agent wizard.
4. Click "Next", and then navigate to your recovery certificate.
5. Click the certificate, and then click "Open".
6. When you are asked if you want to install the certificate, click "Yes", click "Next", and then click "Finish".
7. Open a Command Prompt.
8. At the command prompt, type "gpupdate /force", and then press "Enter".
Bitlocker: Starting in Windows 7, Microsoft also offers an option to do full disk encryption. Bitlocker can either use a Trusted Platform Module (TPM) to store the encryption keys, or an external USB device that must be inserted into the machine during boot to load and validate the keys.
Common mistakes that lead to weak cryptography implementations:
• Using a standard modulus in RSA which is too small. (The small modulus makes cryptanalysis easier)
• Using seeds for symmetric algorithms that are not random enough
• Hard coded cryptographic secrets/elements
• Using too short a key
• Re-using keys
• Unsecure Key Escrow
• Use of an unsecure cryptographic block mode such as ECB mode
• Use of proprietary cryptographic algorithms
Steganography: the hiding of a secret message within an ordinary message and the extraction of
it at its destination. Most common implementation is through the use of Least Significant Bit (LSB) replacement.
Payload: the data to be covertly communicated.
Carrier: the signal, stream, or data file into which the payload is hidden.
Channel: the type of medium used. This may be still photos, videos, or sound files.
Steganalysis: analysis of an image to detect the use of steganography. Two common types are:
Raw Quick Pair (RQP) method: based on statistics of the numbers of unique colors and closecolor
pairs in a 24-bit image. RQP analyzes the pairs of colors created by LSB embedding.
Chi-Square Analysis: measures the theoretical versus calculated population difference of the bits.
The National Security Agency (NSA) cryptography suites:
Suite "A" is classified
Suite "B" is publicly available
Algorithms are classified by type as well - Type 1 - Type 4 (Type 1 is the highest classification)
Type 1 - Juniper (block cipher), MAYFLY (asymmetric), FASTHASH (hashing), WALBURN (high bandwidth link encryption), PEGASUS (satellite telemetry)
Type 2 - Skipjack, Key Exchange Algorithm (KEA)

Type 3 - DES, 3-DES, SHA, AES (some AES implementations are considered Type 1)
Type 4 - Not certified for any gov't usage
Commercial NSA (CNSA) suite includes cryptographic algorithms for encryption, hashing, digital signatures and key exchange:
Encryption: Advanced Encryption Standard (AES) - FIPS 197
Hashing: Secure Hash Algorithm (SHA) - FIPS 180-4
Digital Signature: Elliptic Curve Digital Signature Algorithm (ECDSA) - FIPS 186-4
Digital Signature: RSA - FIPS 186-4
Key Exchange: Elliptic Curve Diffie-Hellman (ECDH) - NIST SP 800-56A
Key Exchange: Diffie-Hellman (DH) - IETF RFC 3526
Key Exchange: RSA - NIST SP 800-56B rev 1

Episode Title: Cryptanalysis
Cryptanalysis is the art or process of deciphering coded messages without being told the key.
Frequency Analysis: examining ciphertext looking for patterns that can be examined against the frequency rate of letter usage by language.
Kasiski test: A variation on frequency analysis that is used to attack polyalphabetic substitution ciphers.
Chosen Plaintext Attack: attacker obtains the ciphertexts corresponding to a set of plaintexts. This can allow the attacker to attempt to derive the key used and thus decrypt other messages encrypted with that key.
Ciphertext Only Attack: attacker ONLY has access to the ciphertext of messages.
Related-Key Attack: Similar to the Chosen Plaintext Attack, except that the attacker is able to get
messages encrypted with two different keys (the keys need to be related, meaning that one was derived from the other as is the case in wireless systems)
Linear Cryptanalysis: a known plaintext attack and uses a linear approximation to describe the behavior of the block cipher. Given sufficient pairs of plaintext and corresponding ciphertext, bits of information about the key can be obtained and increased amounts of data will usually give
a higher probability of success. Invented by Mitsarue Matsui.
Differential Cryptanalysis: a form of cryptanalysis applicable to symmetric key algorithms. This was invented by Eli Biham and Adi Shamir. The examination of differences in an input and how that affects the resultant difference in the output.
Integral Cryptanalysis: Similar to Differential Cryptanalysis, but uses a different technique. Uses sets or even multisets of chosen plaintexts of which part is held constant and another part varies through all possibilities.
What are the three resources required to perform Cryptanalysis?
Time | Memory | Data
How we measure success:
• **Total break** - attacker gets the key.
• **Global deduction** - attacker discovers a functionally equivalent algorithm for encryption and decryption, but without learning the key.
• **Instance (local) deduction** - attacker discovers additional plaintexts (or ciphertexts) not previously known.
• **Information deduction** - attacker gains some information about plaintexts (or ciphertexts) not previously known.
• **Distinguishing algorithm** - attacker can distinguish the cipher from a random permutation.
Password cracking and Rainbow Tables - http://project-rainbowcrack.com/table.htm