Cryptography=To protect transmitted info from being read and understood by anyone but the recipient.

Definitions

**Block Cipher.** Obtained by segregating plaintext into blocks or bits and applying the identical encryption algorithm and key to each block.

**Cipher.** A cryptographic transformation that operates on characters or bits

**Ciphertext or Cryptogram.** An unintelligible message.

**Clustering.** A situation in which a plaintext message generates identical ciphertext messages by using the same transformation algorithm, but with different cryptovariables or keys.

**Codes.** A cryptographic transformation that operates at the level of words or phrases.

**Cryptanalysis.** The act of obtaining the plaintext or key from the ciphertext that is used to obtain valuable info to pass on altered or fake messages in order to deceive the original intended recipient; breaking the ciphertext. AKA: The science of breaking codes

**Cryptographic Algorithm.** A step by step procedure used to encipher plaintext and decipher ciphertext.

**Cryptology.** Encompasses cryptography and cryptanalysis. Cryptology is cryptography and cryptanalysis

**Cryptography.** Science of codes
**Padding** - meaningless data added to start and end of message to hide true length!

**End to end encryption.** Encryption of data from source system to end system (https). In symmetric key encryption, this requires the sender and receiver to have the identical key for the session.

**Key or Cryptovariable.** Info or a sequence that controls the enciphering and deciphering of messages.

**Link Encryption** Individual application of encryption to data on each link of a network. Each entity has keys in common with its two neighboring nodes in the transmission chain.

**One time pad** Usually implemented as a stream cipher using the XOR function. The key has the same length of the message. It is used once and never again. Unbreakable. Invented by Mauborge of army and gilerbert vernam of at&t.

**Stenanography.** Secret communications where the existence of the message is hidden.

**Work function(factor)**. The difficulty in recovering the plaintext from the cipher as measured by cost and time.

**Key clustering.** When 2 different keys encrypt a plaintext message into the same ciphertext.

**Monoalphabetic substitution** When one alphabet is used. Caesar used this.

**Diffusion.** The purpose of diffusion is to spread the influence of a plaintext character over many ciphertext characters. Diffusion can be implemented by means of a Product Cipher.
**Polyalphabetic Cipher.** Accomplished through the use of multiple substitution ciphers.

**MD5-**
An algorithm created in 1991 by Professor Ronald Rivest that is used to create digital signatures. It is intended for use with 32-bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

---

**Notes to remember**

**Private key** is 1000 or more times faster than public key

**Time stamps** can be used to prevent replay attacks.

**One time pad** is usually implemented as a stream cipher using XOR function

**Security of cryptosystem** should only depend on security of keys, not the algorithm.

**Unix systems** use a substitution cipher called ROT 13

---

**Classical Ciphers**

**Substitution**

The Caesar cipher is an example of this. It involves shifting the alphabet 3 positions to the right. The Caesar Cipher is a subset of the Vigenere polyalphabetic cipher Vulnerable to frequency analysis attacks.

**Transposition (permutation)**
Another type of cipher. In this cipher, the letters of the plaintext are permuted. This cipher is also vulnerable through frequency analysis, but it hides the statistical properties of letter pairs and triples such as “IS” and “TOO”

**Vernam Cipher (one time pad) by AT&T**

Implemented through a key that consists of a random set of non repeating characters. Length of the key character stream is equal to full length of message. For megabyte and gig messages, this cipher isn’t practical.

**Book or Running Key Cipher**

This cipher uses text from a source, say a book to encrypt plain text. Attacked by exploiting redundancy in the key

**CODES**

**Steganography**

The art of hiding the existence of a message. Can be used to make a digital watermark to detect illegal copying of digital images.
Secret Key cryptography (symmetric) aka conventional

Familiar to most people. Sender and receiver both know key. Good for data that’s not going anywhere. Sender encrypts the plaintext message with secret key, receiver decrypts same message with same key. For increased security, the secret key should be changed at frequent intervals.

An important property of any secret key cryptographic system is that the same key can encipher and decipher the message.

One problem with symmetric key is that because the sender and receiver must share the same secret key, the sender requires a different key for each intended receiver. Time stamping is a counter to replay. Symmetric key systems however do not provide mechanisms for authentication and non repudiation. DES is the most popular symmetric key system. Though I’ve listed several others.

DES
The algorithm this standard uses is an IBM made algorithm. DES is used for commercial and non-classified purposes.
Devised in 1972 as a derivation of the Lucifer algorithm.
DES describes DEA. Will be replaced by AES eventually.
DEA uses 64 bit block size and a 56 bit key.
-Uses 16 rounds of transposition and substitution
A DES key sequence is 8bytes long

DES operates in 4 modes:
1. Cipher block Chaining-good for authentication
2. electronic Code Book
3. Cipher feedback-good for authentication
4. Output feedback

CipherBlocking Chaining- operates with plaintext blocks of 64 bits. Random generated 64 bit initialization vector is XORed with the first block of plaintext used to disguise the first part of the message that is predictable. Known for errors

ElectronicCodeBook- Native mode of DES and is a block cipher best suited for use with small amounts of data. Usually applied to encrypt initialization vectors or encrypting keys.
**CipherFeedbackMode**- A stream cipher where the ciphertext is used as feedback into the key generation source to develop the next key stream. Here, the ciphertext has equal amount of bits as plaintext. Errors propagate in this mode.

**Output feedback**- A stream cipher that generates the ciphertext key by Xoring the plaintext with a key stream. Feedback is used to generate the key stream, therefore the key stream varies. No errors.

**Triple DES.**
Encrypt with first key, decrypt with second key, encrypt with first key. Encrypting only twice offers no more protection than single DES.

**AES**
This will eventually replace triple DES. NIST announced a competition to choose the algorithm the Advanced Encryption Standard would utilize. The algorithm chosen was the Rijndael Block Cipher.

**The Rijndael Block Cipher**
Designed to have the following properties:
- resistance against all known attacks
- design simplicity
- code compactness and speed

Can be categorized as an iterated block cipher with a variable block length and key length that can be independently chosen as 128, 192, or 256 bits.

Rijndael cipher employs a round transformation that is comprised of three layers of distinct and invertible transformations.

The 3 layers are:
- non linear
- linear mixing
- key addition

The Rijndael block cipher is suited for the following types of implementations:
- high speed chips with no area restrictions
- a compact co-processor on a smart card.
The **twofish algorithm**
A symmetric block cipher that operates on 128bit blocks in 16 rounds that works in all standard modes. Can accept key lengths up to 256 bits.

Employs what is termed as “prewhitening” and “post whitening” where additional subkeys are XORed with the plaintext before the first round and after the sixteenth round. In twofish algorithm, the MDS matrix, the PHT, and key additions provide diffusion.

The **IDEA cipher**
A secure, secret, key block encryption algorithm developed by Massey/Lai. Operates on 64-bit plaintext blocks and uses a 128 bit key. Applies both confusion and diffusion. IDEA performs 8 rounds and operates on 16bit sub blocks. With its 128bit key, its much more difficult to crack than DES. Applied to PGP

**RC5**
A family of cryptographic algorithms invented by Ronald Rivest. A block cipher of variable block length, encrypts through integer addition, the application of a bit wise Exclusive Or, and variable rotations. The key size and number of rounds are also variable. # of rounds can range from 0-255. Typical block sizes are 32, 64, or 28 bits.

Hybrid systems-USES PRIVATE KEY FOR ENCRYPTION OF MESSAGE!

**Public (asymmetric) key cryptosystems**
Public key systems employ two keys, a public key and a private key. The public key is made available to anyone wanting to encrypt and send a message. The private key is used to decrypt the message. The following are important points to note:

- The public key cannot decrypt the message that is encrypted
- Ideally, the private key cant be derived from the public key
- A message that is encrypted by one of the keys can be decrypted with the other
- The private key is kept private.
**One way functions**

Public Key cryptography is possible through the application of a one way function. A one way function is a function that is easy to compute in one direction, yet is difficult to compute in the reverse. For a one way function to be useful in the context of public key cryptography, it should have a **trapdoor**. A trapdoor is a secret mechanism that enables you to easily accomplish the reverse function in a “one way function” scenario.

**Public Key Algorithms**

A number of algorithms have been developed. Some of these are applicable to digital signatures, encryption, or both.

**RSA**

RSA algorithm factors large numbers. This algorithm is based on the difficulty of factoring a number, which is the product of two large prime numbers. These numbers may be 200 digits each.

RSA can be used for encryption, key exchange, and digital signatures.

**Diffie-Hellman Key exchange (1976)**

Yet another algorithm. This is a method where subjects exchange secret keys over a nonsecure medium without exposing the keys. This method enables two users to exchange a secret key over an insecure medium without an additional session key. It consists of 2 public parameters.

**El Gamal (1985)**

Dr Gamal extended the Hellman concepts to apply to encryption and digital signatures. El gamal is a non patented public key cryptosystem that is based on the discrete logarithm problem.
**Merkle-Hellman Knapsack**
Is based on the problem of having a set of items with fixed weights and determining which of these items can be added to in order to obtain a given total weight. The concept is that each succeeding term in the set is greater than the sum of the previous terms.

**Elliptic Curve (Koblitz 1986/1987)**
Another approach to public key cryptography. Elliptic curves are usually defined over finite fields such as real and rational numbers and implement an analog to the discreet logarithm problem.

Smaller key sizes in the elliptic curve implementation can yield high levels of security. This means less computational and memory requirements. For ex:, a EC key of 160 bits, equals a 1024 bit RSA key.

That’s why EC is best suited to hardware applications such as smart cards and wireless devices. Elliptic curves can be used to implement digital signatures, encryption, and key management capabilities.

**Public Key Cryptosystems Algorithm Categories**
Public key encryption utilizes hard, one way functions.

The problems with using this type of encryption are:
- Factoring the product of large prime numbers
- Finding the discreet logarithm in a finite field
Digital Signatures

The purpose of digital signatures is to detect unauthorized mods of data, and to authenticate the identity of the signatures and non-repudiation. *A message is said be digitally signed, if it is sent with Message Digest Encrypted with Senders Private Key*

These functions are accomplished by generating a block of data that is usually smaller than the size of the original data. The smaller block of data is bound to original data and to the identity of the sender.

To generate a digital signature, the digital signature program passes the file to be sent through a one way hash function. This hash function produces a fixed size output from a variable size input. The output of the hash function is called a message digest. The message digest is uniquely derived from the input file, and if the hash algorithm is strong, the message digest should have the following characteristics:

- has function considered oneway
- two files shouldn’t have the same message digest
- The message digest should be calculated using all of the original file’s data

After the message digest is calculated, it is encrypted with the sender’s private key. The encrypted message digest is then attached to the original file and is sent to the receiver. The receiver, then, decrypts the message digest using the sender’s public key.

Verification occurs because the sender’s public key is the only key that can decrypt the message digest encrypted with the sender’s private key.
Digital Signature Standard (DSS) and Secure Hash Standard (160bit)

This standard enables the use of the RSA digital signature algorithm or the digital signature algorithm (DSA). The DSA is based on a modification of the El Gamal digital signature.

Both of these digital signature algorithms use the Secure Hash Algorithm. The SHA computes a fixed length message digest from a variable length input message. This message digest is then processed by the DSA to either generate or verify the signature.

Some more on SHA:

- produces a message digest of 160 bits when any message less than 2(64) bits is used as input

- It is computationally infeasible to find a message that corresponds to a given message digest

- it is computationally infeasible to find two different messages that produce the same message digest.

- The length of the message is the number of bits in a message

MD5

A message digest algorithm. MD5 takes a message of an arbitrary length and generates a 128 bit message digest. In MD5, the message is processed in 512 bit blocks in four distinct rounds.
A SUMMARY OF SENDING A MESSAGE WITH DIGITAL SIGNATURE

1. A hash algorithm is used to generate the message digest from the message.

2. The message digest is fed into the digital signature algorithm that generates the signature of the message. The signature of the message is accomplished by encrypting the message digest with the sender’s private key and attaching the result to the message. Thus, it is signature.

3. The message and the attached message digest are sent to the receiver. The receiver then decrypts the attached message digest with sender’s public key. The receiver also calculates the message digest of the received message using the identical hash function as the sender. The 2 message digests should be identical.

Hashed Message Authentication Code

An HMAC is a hash algorithm that uses a key to generate a message authentication code. A MAC is a type of checksum that is a function of the info in the message. The mac is generated before the message is sent, appended to the message, and then both are transmitted.

At the receiving end, a MAC is generated from the message alone using the same algorithm as used by the sender, and this mac is compared to the mac sent with the message.
Hash Function characteristics

Used to condense a message of an arbitrary length, into a fixed length message digest. This message digest should uniquely represent the original message, and it will be used to create a digital signature. Furthermore, it should NOT be computationally possible to find two messages.

Cryptographic Attacks

Cryptanalysis is used to obtain valuable info and to pass on altered or fake messages in order to deceive the original intended recipient.

Brute force- tries every possible combo

Known Plaintext The attacker has a copy of the plaintext corresponding to the ciphertext.
**Chosen Plaintext** Chosen plaintext is encrypted and the output ciphertext is obtained.

**Adaptive Chosen Plaintext.** A form of a chosen plaintext attack where the selection of the plaintext is altered according to the previous results.

**Ciphertext only-**Only the ciphertext is available

**Chosen ciphertext.** Portions of the ciphertext are selected for trial decryption while having access to the corresponding decrypted plaintext.

**Adaptive Chosen Ciphertext.** A form of a chosen ciphertext attack where the selection of the portions of ciphertext for the attempted decryption is based on the results of previous attempts

**Birthday Attack.** Usually applied to the probability of two different messages using the same has function that produces a common message digest; or given a message and its corresponding message digest, finding another message that when passed through the same has function generates the same specific message digest.

**Meet in the middle** Applied to double encryption schemes by encrypting known plaintext from one end with each possible key and comparing the results “in the middle” with the decryption of the corresponding ciphertext with each possible key.

**Man in the middle** An attacker taking advantage of the store and forward nature of most networks by intercepting messages and forwarding modified versions of the original message while in between two parties attempting secure communications.
**Differential Cryptanalysis** Applied to private key cryptographic systems by looking at ciphertext pairs, which were generated through the encryption of plaintext pairs, with specific differences and analyzing the effect of these differences.

**Linear Cryptanalysis.** Using pairs of known plaintext and corresponding ciphertext to generate a linear approximation of a portion of a key

**Differential Linear Cryptanalysis.** Using both differential and linear approaches.

**Factoring.** Using a mathematical approach to determine the prime factors of large numbers.

**Statistical** Exploiting the lack of randomness in key generation.
Public Key Certification systems

A source that could compromise a public key cryptographic system is an individual “A” who is posting a public key under the name of another individual “B”. In this scenario, the people who are using this public key to encrypt the messages that were intended for individual B will actually be sending messages to individual A. Because individual A has the private key that corresponds to the posted public key, individual A can decrypt the message that were intended for individual B.

Digital Certificates
To counter this attack, a certification process can be used to bind individuals to THEIR public keys. A Certificate Authority (CA) acts as notary by verifying a persons identity and issuing a certificate that vouches for a public key of the
named individual. This certification Agent signs the certificate with its own private key. Therefore, the individual is verified as the sender if that person’s public key opens the data.

The certificate contains the subjects name, public key, and name of the certificate authority, and the period in which the cert. Is valid.
To verify the CA’s signature, its public key must be cross certified with another CA. This cert. Is then sent to a Repository, which holds the Certificates and Certificate Revocation Lists that denote the revoked certificates.

------------------------------
------------------------------

Public Key Infrastructure (PKI)
The integration of digital signatures and certificates, and the other services required for E-commerce is called the Public EY Infrastructure. These services provide integrity, access control, confidentiality, authentication, and non repudiation for electronic transactions. All these certificates are stored in something called an LDAP. Anyway…. The PI includes the following elements:

*Digital certificates, certificate authority, registration authorities, policies and procedures, certificate revocation, non repudiation support, timestamping, LDAP, security enabled applications, cross certification.*

The LDAP (aka: certificate directory server) provides a standard format to access the certificate directories. The primary security concerns relative to LDAP servers are availability and integrity. For example: a DOS attack could prevent access to the Cert Revocation List, and thus permit the use of a revoked cert for transactions.
Anyway, the LDAP servers on a network and the servers on this network provide public keys and corresponding X.509 certs for the enterprise. A directory contains the info like: Names, addresses, phone numbers, public key certs.

**Approaches to Escrowed Encryption**

In some cases, there is need for agencies to have access to information transmitted electronically over computer networks. To have this access, agencies need the encryption keys to read the enciphered messages. At the same time, the privacy of citizens must be protected from illegal and unauthorized surveillance of their digital communications.

**The Escrowed Encryption Standard**

The idea is to divide the key into two parts, and to escrow two portions of the key with two separate trusted organizations. Then, agencies, after obtaining the court order, can retrieve the two pieces of the key from the organizations to decrypt the message.

The escrowed encryption standard is embodied in the US governments Clipper Chip, which is implemented in tamper proof hardware. The skipjack secret key algorithm performs the encryption.

Each clipper chip has a unique serial number and an 80 bit unique unit or secret key. The 80 bit key of the clipper chip is weak.
Another key escrow approach is fair cryptosystems. Here, the private key of a public/private key pair is divided into multiple parts and distributed to different trustees. One valuable characteristic approach is that each portion of the secret key can be verified as correct without having to reconstruct the entire key. This is accomplished by giving each trustee a piece of each public key and private key. If authorities have the legal permission to decrypt a message that is encrypted with the secret key, they can obtain all the portions of the private key and read the message.

This concept can be applied by voluntary trustees in different countries or business areas …rather than government agencies.

Key Management Issues.
Obviously when dealing with encryption keys, the same precautions must be used as with physical keys to secure the areas or the combinations to be safes. These precautions include:
Email security issues and approaches (never store permanent records in email directory!!!)

The main objectives of email security are to ensure the following:
- non repudiation
- messages are read by only intended recipients
- integrity of message
- authentication of the source
- verification of delivery
- labeling of sensitive material
- control of access

The following standards have been developed to address some or all of these: (next page)

1. Secure Multipurpose Internet Mail
A specification that adds secure services to email in a MIME format. Provides authentication through digital signatures and the confidentiality of encryption. Follows public Key cryptography standards and uses X.509 for digital signatures.
2. **MIME object security services**
   Provides flexible email security services by supporting different trust models. Provides authenticity, integrity, confidentiality, and non repudiation. Uses MD2/MD5, RSA, and DES.

3. **Privacy Enhanced Mail (PEM) - Uses DES**
   A standard proposed by IETF to be compliant with the Public Key Cryptography Standards which were developed by MS, Novell, and SUN. Supports the encryption and authentication of internet email. Uses triple DES.

4. **PGP - a hybrid system**
   Symmetric cipher IDEA (international data encryption algorithm) used to encipher message, RSA used to symmetric key exchange and for digital signatures. Instead of certificate authority, pgp uses a web of trust. Users can certify each other in a mesh model. Uses symmetric algorithm to encrypt data, and uses an asymmetric system to encrypt and exchange secret keys.

### Internet security applications

1. **Message authentication code (MAC) or the financial institution message authentication standard (FIMAS)**

   In order to protect against fraud in electronic fund transfers, the MAC, ANSI X9.9 was made. The MAC is a check value, which is derived from the contents of the message itself. A MAC is appended to the message before it is transmitted. At
the receiving end, a MAC is generated from the received message and compared to the MAC of the original message. To strengthen the MAC algorithm, a keyed MAC can be generated using DES.

2. **SET**
Developed in 1997 as a means of preventing fraud. Provides confidentiality for purchases by encryption of payment info. Uses DES symmetric key system for encryption of the payment info and uses RSA for the symmetric key exchange and digital signature. SET covers the end to end transactions from the cardholder to the financial institution. SET requires 2 pairs of asymmetric keys and 2 digital certificates!

3. **SSL/TSL**
Supports RSA public key algorithms, IDEA, DES, and 3DES private key algorithms, and the MD5 has function. SSL 3.0 and its successor, the transaction layer security protocol are defactor standards, but do not provide end to end capabilities of SET. Provides confidentiality, authentication, and integrity, above the transport layer. TLS, as with SSL, can be used with applications such as telnet, ftp, http, and email protocols. Both use certificates for public key verification.

4. **Internet Open Trading Protocol**
An Internet protocol that is aimed at the consumer to business transactions. Similar to shopping in the real world. Gives buyers the option to choose method of payment. Supports public and private encryption key algorithms and can use digital certificates. Flexible and can accommodate future payment models.

5. **Mondex**
This system is an example of a cash smart card application. The value of the amount of currency is stored in smart cards
and a proprietary encryption algorithm provides security. Because the algorithm is not subject to public scrutiny, its strength and vulnerabilities are not known. The smart card then, can be used in financial transactions instead of cash. If card is lost, finder can use it as cash.

6. IPSEC
A standard that provides encryption, access control, and non repudiation over an IP. The 2 main protocols of Ipsec are AH and ESP.
AH provides integrity, authentication, and non repudiation. An esp primarily provides encryption, but also limited authentication.

At the heart of IPSec is the security association.

IPSEC can operate in transport or tunnel mode. IN transport mode, data in the IP packet is encrypted, but the header is not.

In tunnel mode, the original IP header is encrypted and a new IP header is added to the beginning of the packet.

7. SHTTP
Alternative to SSL. SSL is for entire sessions, SHTTP can be used to protect individual WWW documents. Provides authentication, confidentiality, integrity, and non repudiation. Supports a wide variety of encryption algorithms.

8. SSH2
Provides confidentiality and integrity services. Comprised of a transport layer protocol, user authentication protocol, and
connection protocol. Used to authenticate the client to the server.

**Wireless Security**

Some issues:
- physical security of devices themselves
- Proliferation of many different platforms
- protection of sensitive financial transactions
- limitations of processing power and memory due to space and weight considerations
- no standard method for securing wireless transactions.
- Public Key Infrastructure.

**WAP.**

Aimed at small displays and systems with limited bandwidth. Not designed to display large volumes of data on a small mobile display.

WAP security uses WIRELESS TRANSPORT LAYER SECURITY PROTOCOL

1. Class 1 (anonymous authentication) The client logs on to server, but neither client or server can be certain of identity of each other

2. Class 2 (server authentication). The server is authenticated to the client, but the client is not authenticated to the server

3. Cass 3 (two way client and server authentication) The server is authenticated to the client and the client is authenticated to the server
Authentication and authorization can be performed on the mobile device using smart cards to execute PKI enabled transactions.

What is **Wap Gap**?
Results from the requirement to change security protocols at the carriers WAP gateway from the wireless WTLS to SSL for use over the wired network. At the WAP gateway, the transmission, which is protected by WTLS, is decrypted and then re-encrypted for transmission using SSL. Thus the gap occurs.

**The IEEE 802.11 wireless standard**
A wireless LAN standard that specifies an interface between a wireless client and base station or access point, as well as among wireless clients.

**802.11 layers**
The IEEE 802.11 standard places specs on the parameters of both the physical layer and mac layers of the network.

The physical layer is responsible for transmission of data among nodes

Mac layer is a set of protocols responsible for maintaining order in the use of shared medium. The 802.11 standard specified a carrier sense multiple access with collision avoidance.

The mac layer provides the following services:

**Data transfer** – CSMA/CA media access
**Association** – establishment of wireless links between clients and access points in infrastructure networks

**Reassociation**- this action takes place in addition to association when a wireless client moves from one basic service set to another, such as in roaming

**Authentication**- process of proving a client identity through the use of the 802.11 option, WEP. In wep a shared key is configured into the access point and its wireless clients. Only those devices with a valid shared key will be allowed to be associated with the access point.

**Privacy** – data is transferred in the clear by default.

**Power management**- Two power modes are defined in the IEEE 802.11 standard: An active mode used in transmitting and receiving and a power save mode that conserves power but does not enable the user to transmit or receive.