Network Security

Dr. Ihsan Ullah

Department of Computer Science & IT
University of Balochistan, Quetta
Pakistan

March 26, 2015

Cryptography

- Comes from the Greek words **kryptos** (hidden) and **graphos** (writing)
- The use of mathematical operations to protect messages traveling between parties or stored on a computer
- A very important security countermeasure/control
- Encryption for confidentiality was the original purpose of cryptography

Encryption & Decryption

Plaintext

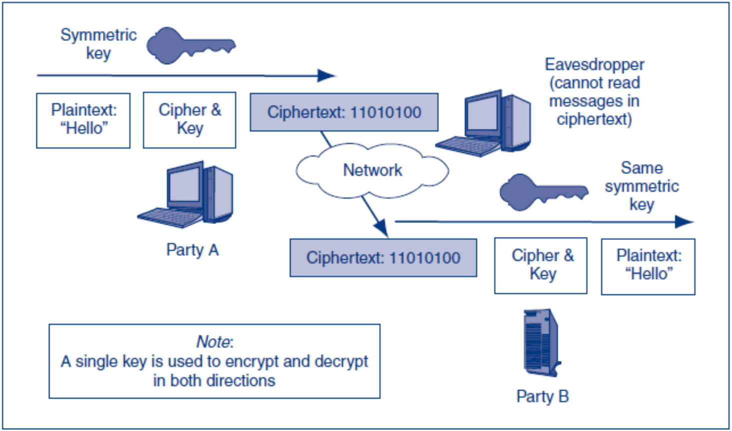
- The original message is called the plaintext
- Got the name when cryptography was only used for text messages
- Today, however, plaintext messages can be images, sounds, videos, or a combination of several data formats

Cryptography

Encryption & Decryption

- Encryption is a cryptographic process that turns the plaintext into a seemingly random stream of bits called the ciphertext
- Ciphertext is also known as encrypted or encoded information because it contains a form of the original plaintext that is unreadable by a human or computer directly
- Ciphertext needs to be decrypted to get back the original plaintext
- Decryption

Encryption & Decryption



Encryption & Decryption

Cipher

- A specific mathematical process used in encryption and decryption
- Many ciphers exist, which operate differently
- The same cipher must be used for both encryption and decryption

Encryption & Decryption

Key

- A random string of bits
- For a given cipher, different keys will generate different ciphertexts from the same plaintext
- The key must be kept secret not the cipher
- $C = E(P, K)$, where C is the ciphertext, E is the encryption algorithm, K is the key and P is plaintex

Substitution cipher

- One character is substituted for another, but the order of characters is not changed
- For example letters in alphabet ABCDEFGHIJKLMNOPQRSTUVWXYZ correspond to CDEFGHIJKLMNOPQRSTUVWXYZAB

Substitution cipher

Caesar Cipher

- Each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet
- Simplest substitution cipher
- For example $C_i = E(P_i, 3) = P_i + 3$
- ABCDEFGHIJKLMNOPQRSTUVWXYZ
- DEFGHIJKLMNOPQRSTUVWXYZABC
- Using this encryption "HELLO" becomes "LHNNR"

Substitution cipher

Variable key

Plaintext	Key	Ciphertext
n	4	r
o	8	w
w	15	l
i	16	...
s	23	...
t	16	...
h	3	...
e	9	...
t	12	...
i	20	...
m	6	...
e	25	...

Transposition ciphers

- Move letters around within a message but characters are not substituted

Example (key 132231)

	Key (part1)		
Key (Part 2)	1	3	2
2	n	o	w
3	i	s	t
1	h	e	t

- Taking the (column number, row number) value out, makes ciphertext
- Values are taken in order (1,1), (1,2), (1,3) ...
- Resulatant ciphertext is “hnitwteos”

Real-world encryption

- Encryption is done on bits not on letters of the alphabet
- Mixing several rounds of both transposition and substitution to give good randomness

Symmetric key encryption

- In symmetric key encryption, a single key is used for encryption and decryption in both directions
- Ciphers discussed so far are symmetric key encryptions
- Nearly all encryptions for confidentiality use symmetric key encryption

Key length

- Only the key needs to be kept secret for successful confidentiality
- One way for an attacker to learn the key is doing an **exhaustive search** – trying all possible keys until the correct one is found
- Longer the key, it takes longer to search all possible keys
- For a key of length N bits, there are 2^N possible keys
- On average, half of the keys must be tried $(2^N/2)$
- Each additional bit in the key doubles the time it will take to crack the key
- A symmetric key that is 100 bits long or longer is considered a strong symmetric key

Symmetric key encryption ciphers

Data Encryption Standard (DES)

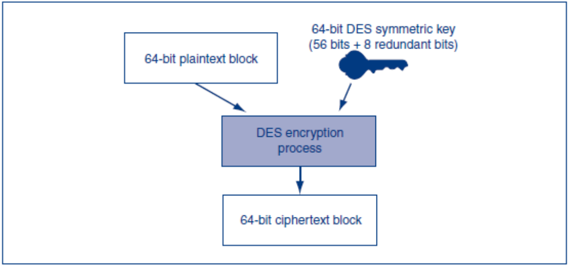
- Created by the U.S. National Bureau of Standards (now called National Institute of Standards and Technology (NIST)) in 1977
- Widely available and supported by hardware accelerators
- Uses a key of 56 bits on 64 bits block sizes
- Block encryption standard [1]
- Key size short for today's most transactions

[1] A block cipher processes the input one block of elements at a time, producing an output block for each input block [Sta10]

Symmetric key encryption ciphers

Data Encryption Standard (DES)

- Abstract working of DES



[BP12]

Symmetric key encryption ciphers

Triple DES (3DES)

- Simply applies DES three times in a row for extra strength
- Normally performed with three different DES keys
- Gives an effective key length of 168 bits (3 times 56)
- **Encrypts** the plaintext block with the **first key**, **decrypts** the output of the first step with the **second key**, and then **encrypts** the output of the second step with the **third key**
- Can also be used with a single shared key (backward compatible with DES)

Symmetric key encryption ciphers

112-BIT 3DES

- A variant of 3DES that uses only two keys
- The third operation of the sender (to encrypt the output of the second stage) is performed with the first key
- Effective key size of 112 bits (2 times 56)

Symmetric key encryption ciphers

3DES usability

- From a security standpoint, 3DES gives strong symmetric key encryption
- From a practical point of view, DES is slow, and having to apply DES three times is very slow and therefore expensive in terms of processing cost

Symmetric key encryption ciphers

Advanced Encryption Standard (AES)

- Released by NIST in response to the weakness in DES (2001)
- Efficient enough in terms of processing power and RAM requirements to be used on a wide variety of devices including cellular telephones
- Offers three alternative key lengths: 128 bits, 192 bits, and 256 bits
- Block cipher: works on 128 bits blocks of plaintext inputs
- Many cryptographic systems now support AES
- AES should dominate encryption for confidentiality in the near future

Symmetric key encryption ciphers

RC4

- A stream cipher[2], designed by Ron Rivest in 1987
- Variable key-size (40 bits or more) stream cipher with byte-oriented operations
- Extremely fast and uses only a small amount of RAM
- National export restrictions in many countries once limited commercial products to 40-bit encryption. Consequently, 40-bit RC4 became the standard key length for WEP (Wired Equivalent Privacy)
- Requires proper implementation, otherwise provides minimal protection

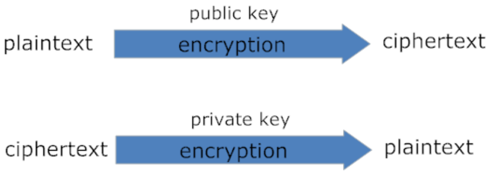
[2] Stream cipher processes the input elements continuously, producing output one element at a time as it goes along [Sta10]

Symmetric key encryption ciphers

	RC4	DES	3DES	AES
Key length (bits)	40 or more	56	168	128, 192, 256
Key strength	Very weak at 40 bits	Weak	Strong	Strong
Processing requirements	Low	Moderate	High	Low
RAM requirements	Low	Moderate	Moderate	Low

Public key cryptography

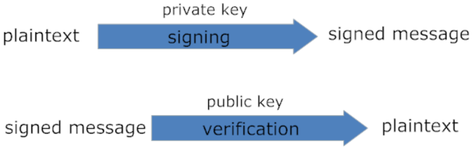
- Also called asymmetric cryptography
- Uses two keys: public key and private key
- Each individual has both the keys where private key is not shared while public key is shared
- RSA[3], DiffieHellman, Digital Signature Standard (DSS) and elliptic-curve



[3] Ron Rivest, Adi Shamir and Leonard Adleman

Public key cryptography

- Can also be used for digital signature
- Digital signature is the encryption of message through private key



Public key cryptography versus symmetric key cryptograhpy

- Public key cryptography can do any thing symmetric key cryptography can do
- In general, public key cryptographic algorithms are far slower than symmetric key cryptographic algorithms
- Often both systems are combined to be used together (public key in the beginning of communication for authentication and securely sharing the secret key)

Hash algorithms

- Also known as message digests are one way transformations
- A hash function is a mathematical transformation that computes a fixed-length code ($h(m)$) from a message (m) of arbitrary length
- Hashing is an irreversible process
- Does not require a secret key
- Secure Hash Algorithm (SHA3) and Message Digest (MD5)

Properties of hash functions

1. For any message m it is relatively easy to compute $h(m)$, making both hardware and software implementations practical
2. Given $h(m)$, there is no way to find m that hashes to $h(m)$ in way that is substantially easier than going through all possible values of m and computing $h(m)$ for each of them
3. It is computationally infeasible to find two different values that hash to the same thing

Uses of hash functions

Password hashing

- Passwords must be hashed and then stored or transmitted
- Long passwords and uncommon words

Message integrity

- Hash functions can generate a message integrity code (MIC) to be sent along-with the message
- Does not provide integrity alone; message can be intercepted, modified and the hash recomputed
- Using a secret password between the sender and receiver and re-hashing the MIC+password protects against such attacks
- Also called Message Authentication Code (MAC)

Uses of hash functions

Message fingerprint

- To monitor the modification of a large data structure such as a program
- Hash of the data structure is stored and it is periodically compared with newly computed hashes

Digital signature efficiency

- Digital signature over complete message through public key cryptography is costly
- Using public key cryptography over the hash of the message improves efficiency of digital signature

Randy J Boyle and Raymond R. Panko.
Corporate Computer Security (3rd Edition).
Prentice Hall Press, 3rd edition, 2012.

William Stallings.
Network Security Essentials: Applications and Standards.
Prentice Hall Press, Upper Saddle River, NJ, USA, 4th edition, 2010.