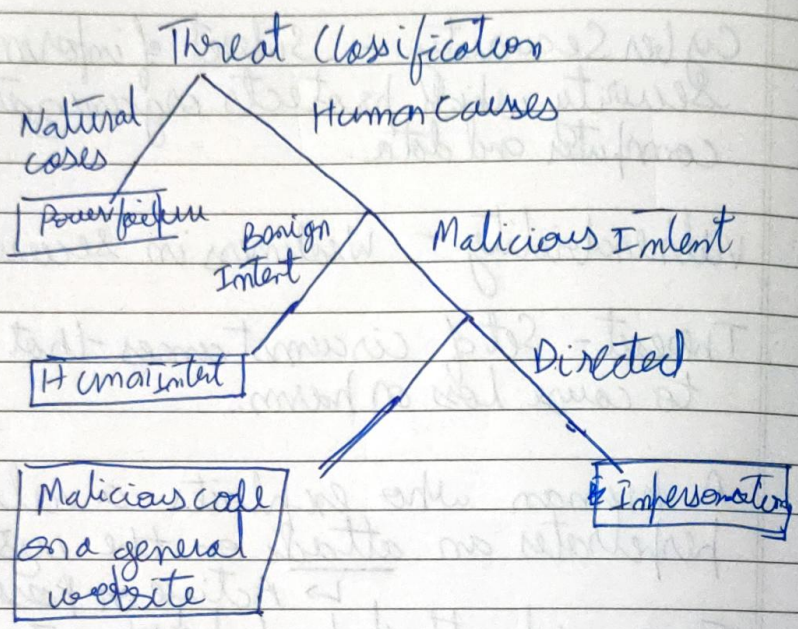
Date: / /

Intro

- Cyber Security - Subset of information Security which protects organization networks, computer and data.
- Vulnerability - Weakness in security system
- Threat - Set of circumstances that has potential to cause loss or harm.
- A human who exploits a vulnerability perpetrates an attack on the system
  - ↳ Active or Passive
- To avoid attacks/vul. | Modifies system
  i) Control as a protective measure
  ii) That is a control is an action, device, procedure or technique that removes or reduces a vulnerability.

C-I-A Triad

- Confidentiality - The ability of a system to ensure that an asset is only viewed by authorised parties
- Integrity - The ability of a system to ensure that an asset is modified only by authorised parties.
- Availability - The ability of a system to ensure that an asset can be used by any authorised parties.



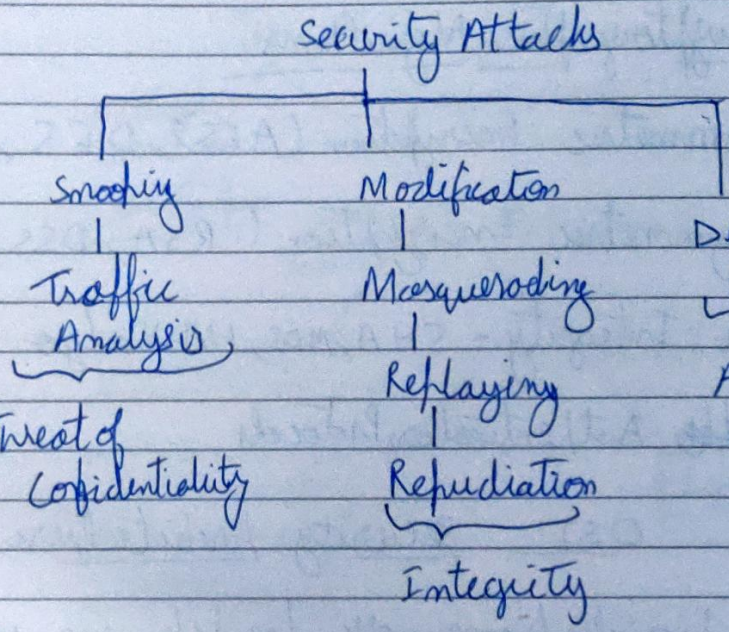
- Computer Security - The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of info system resources
- Authenticity - Property being genuine and able to verify and trust
- Accountability - Security goal that generates the requirements for actions to be traced uniquely.
- Confidentiality - Preserving authorized restrictions on information access and disclosure - protects personal privacy.
- Integrity - guarding against improper destruction and modification

Cryptographic Algorithms

1) Symmetric Encryption (AES, DES, IDEA)
2) Asymmetric Encryption (RSA, DSS, ECC)
3) Data Integrity - SHA, MD5, HASH algo
4) Authentication Protocols

OSI Security Architecture

- OSI provides framework for defining security attacks, mechanisms and services.
- security attacks any action compromises security of information owned by organisation
- A security mechanism is any process designed to detect prevent or recover from a security attack
- Security services a processing or communication that enhance the security of data processing system and information transfers of an organization
- The generic name for the collection of tools designed to protect data and thwart hackers is computer security



- Passive Attacks - Methods such as ~~eavesdropping~~ eavesdropping
Two types - Traffic Analysis and release of message contents
- Passive attacks don't invoke any alteration of data

Active Attack:

1) Masquerade - One entity pretends to be another
2) Replay - The passive capture of a data unit and its subsequent transmission to produce an unauthorized effect
3) Modification of messages: The portion of legitimate message is altered.
4) Denial of service: Prevention or inhibiting the normal use or management of comms facilities

General categories of security Attacks

- Interruption - Attack on availability
- Interception - Attack on confidentiality
- Modification - Unauthorized party gets access. Attack on integrity.
- Fabrication - Inserting counterfeit objects into the system. Attack on authenticity.

Security Services

- Authentication - The assurance that the communicating entity is the one it claims to be.
  → Peer Entity Auth. and Data origin auth.
- Access control - The prevention of unauthorized use of a resource
- Data confidentiality - The protection of data from unauthorized disclosure. Types → connection, connectionless, selective - Field and Traffic Flow.
- Data Integrity - The assurance that data received are exactly as sent by an authorized entity - connection Integrity with / without recovery.
- Non Repudiation - Provides protection against by one of the entities involved in a communication of having in all part of communication.

Security Mechanisms

1) Encipherment - The use of mathematical algorithms to transform data

2) Digital Signature - Data appended to, or a cryptographic information of a data unit that allows recipient of the data unit to prove the source and integrity of data unit and protect against forgery.

3) Access control - A variety mechanism that enforce access rights to resources.

4) Data Integrity - A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

- Kerchkoff's Principle - One should always assume that the adversary knows the encryption/decryption algorithm. The key must be kept secured and secrecy must be maintained.

5) Authentication Exchange - A mechanism intended to ensure the identity of an entity by means of information exchange.

6) Traffic Padding - The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts

7) Routing Control - Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.

8) Notarization - The use of a trusted third party to assure certain properties of data exchange.

Five Ingredients of Symmetric Encryption

1) Plaintext
2) Encryption Algo
3) Secret key
4) Cipher text
5) Decryption Algorithm

- Original message - Plain Text. Coded message cipher text.
- Enciphering - encryption
- Deciphering - decryption
- The schemes used for encryption constitute the area of study known as cryptography.
- Deciphering a message without any knowledge of the enciphering details is cryptanalysis
- The areas of cryptology and cryptanalysis together are called cryptology.

Cryptographic Systems

The three dimensions are:

I) Ciphering methods:
All encryption algos based on two general principles:
i) Substitution: in which each element in the plain text is mapped into another element
ii) Transposition in which elements of plain text are rearranged.

II) The number of keys used
- If both sender and receiver use the same key, the system is refered to as symmetric encryption.

- If sender and receiver used different keys, system is refered to as asymmetric, two-key, or public-key encryption.

III) The way in which the plaintext is processed
- A block cipher processes the input one block of elements at a time an output block for each input block.

- A stream cipher processes the input elements continuously, producing output one element at a time as it goes along.

Cryptanalysis and Brute Force attack

1) Cryptanalysis - Cryptanalysis attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext-ciphertext pairs.

2) Brute-force attack - The attacker tries every possible key on ciphertext until an intelligible translation into plaintext is obtained.

Unconditionally Secured & computationally secured encryption schemes.

- The encryption algorithm should meet one or both following criteria:
  - The cost of breaking the cipher exceeds the value of the encrypted information.
  - The time required to break the cipher exceeds the useful lifetime of the information.

- If both above criteria are met, such an encryption scheme is said to be computationally secure.

- A substitution cipher replaces one symbol with another.

- In monoalphabetic substitution, the relationship between a symbol in the plaintext to symbol in ciphertext always one-to-one.
  Ex: hello -> KHOOR

- Shift cipher or Caesar cipher → Additive cipher where each letter is moved certain no. of word.
- When cipher is additive, the plaintext, ciphertext and key are integers in Z_{26}
- Additive ciphers are also called as shift ciphers. ~~Coss~~ Caesar used a key of 3 for his communications

Substitution Ciphers (Playfair Ciphers)

- The 'key' for a playfair cipher is generally a word.

1) Repeating plaintext letters that are in same pair are separated with filler letter, such as x, so that feel would be treated as fe lx ls.

2) Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with first element of the row circularly from last. For example ~~dm~~ is encrypted as ~~RM~~.
AR ↓ RM

ex: MONARCHY →

5 x 5

m	o	n	a	r
c	h	y	b	d
e	f	g	i/j	k
l	p	q	s	t
u	v	w	x	z

combined because 5x5 matrix

3) 2 plaintext that fall in same column are replaced by letter beneath with top element

ex: MV → CM

4) Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter

ex: he → ~~EE~~ (c, f) lx → ~~QZ~~ (s, v) lo → ~~BX~~ (n, m)

plaintext: hello ciphertext: EC QZ BX

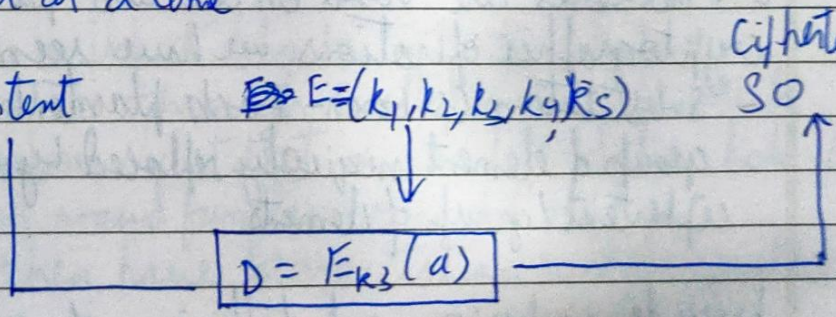
Stream cipher

Call the plaintext stream P, the ciphertext stream C, and the key stream K.

$P = P_1 P_2 P_3 \ldots \quad C = C_1 C_2 C_3 \ldots \quad K = (k_1, k_2, k_3, \ldots)$

$C_1 = E_{k_1}(P_1) \quad C_2 = E_{k_2}(P_2) \quad C_3 = E_{k_3}(P_3)$

★ In stream cipher, encryption/decryption done one symbol at a time



Additive ciphers can be categorized as stream ciphers.

Block Cipher

- In block ciphers, a group of plaintext symbols of size m (m>1) are encrypted together creating a group of ciphertext of the same size.
- A single key is used to encrypt the whole block even if the key is made up of multiple values.

Eg: Playfair ciphers are block ciphers. The size of the ~~last~~ block is m=2. Two characters are encrypted together.

Claude Shanon and Substitution-Permutation ciphers

- Claude Shanon introduced idea of substitution-permutation (S-P) networks
- S-P networks are based on the two primitive cryptographic operations we have seen before
  - Substitution (S-box) - Each plaintext element / group of element uniquely replaced by corresponding ciphertext / group of elements
- Provide confusion and diffusion of message

Confusion and Diffusion

- Cipher needs to completely obscure statistical properties of original message.
- A one-time pad does this
- Combination of both was suggested by Shanon
  i) Diffusion - Dissipates statistical structure of plaintext over bulk of ciphertext
  ii) Confusion - Makes relationship between ciphertext and key as complex as possible

Feistel Cipher Structure

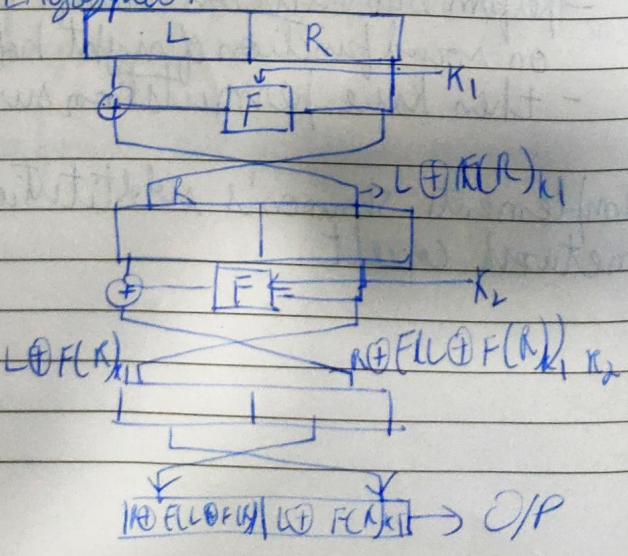
- Horst Feistel devised feistel cipher:
  - based on concept of invertible product cipher.
- Partitions input blocks into two halves
  - Proces through multiple rounds which
  - perform substitution on left data half based on round function of right half.
  - then have permutation swapping values.
- Implements Shanon's substitution-permutations network concept.

Feistel Cipher Design Principles

- block size - Increasing size improves security, but slower.
- key size - Increasing size improves security, makes exhaustive key searching harder, but may slow
- number of rounds - Increasing number improves security, but slows.
- subkey generation - greater complexity can make analysis harder, but slows cipher.
- round function - greater ~~analys~~ complexity can make analysis harder, but slows.
- Fast software en/decryption & ease of analysis - More recent concerns for practical use and testing

~~Conventional Encryption Algorithms~~

Structure Encryption



Pg For decryption use same structure with keys reversed ⊕ XOR reducing undoes first XOR

Conventional Encryption Algorithms

Data Encryption Standard (DES):
- Most widely used
- Block cipher

Plaintext processed in 64-bit blocks
The key is 56 bits in length

At start itself plaintext bits are permuted using an initial permutation.

Hence at end of 16 rounds inverse permutation is applied.

O/P → 64 bit cipher text

Steps:

1) 64 bit text / 64 bit key
2) Initial permutation of 64 bit
3) Round 1 (Total 16) → 64 bit cipher text and 48 bit key input

Key reduction 64 to 48 steps
1) 64 bit to PC1 (Limited choice one)
2) 56 bits enter PC1 as 8 bits removed as parity

3) 2 equal halves (C and D) 28 bits each enter LS
4) Left shift performed depending on round numbers
Round No (1) (2) (9) (16) → 1 bit shift
Otherwise 2 bit shift

5) Now the 2 halves are sent to PC2. From PC2 48 bits are selected which are key input

— x x —

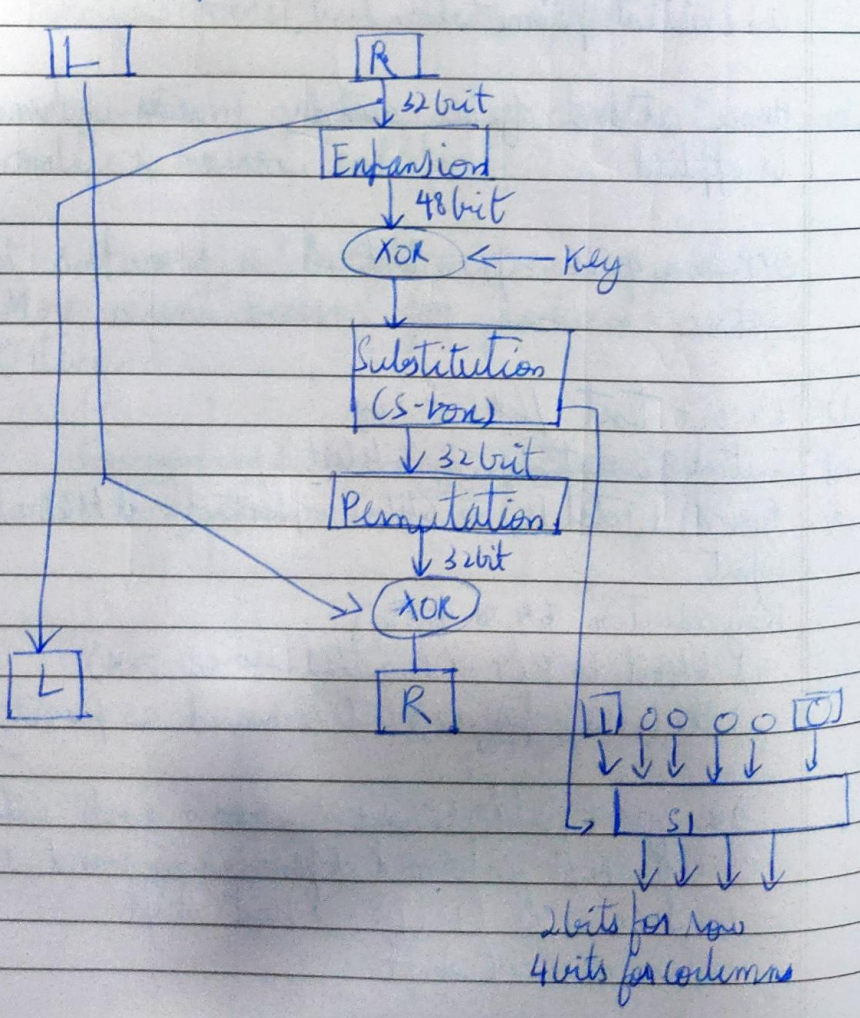
4) Each round new 48 bit key is input.

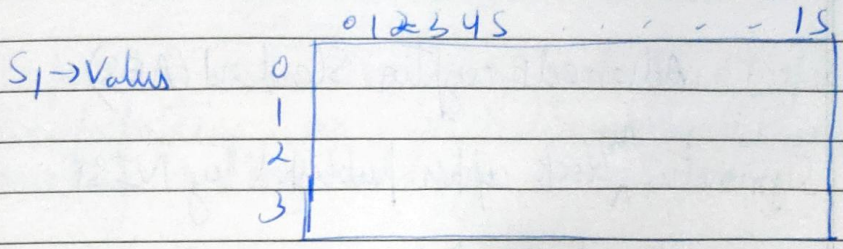
5) After round 16 bits are sent to final permutation (Inverse initial permutation)

6) Ciphertext is obtained

DES ~~round key~~

Functions performed in 16 rounds





S1 values are used to find location in table to obtain value of the cell which is the 4 bit output

- 8 substitution boxes present to obtain 32 bits
- After R16 both the L & R blocks are swapped
- Decryption follows same system with keys in reverse order
- Avalanche Effect - Where a change of one input or key bit results in changing approximately half output bits.
- DES exhibits strong Avalanche effect

Strength:

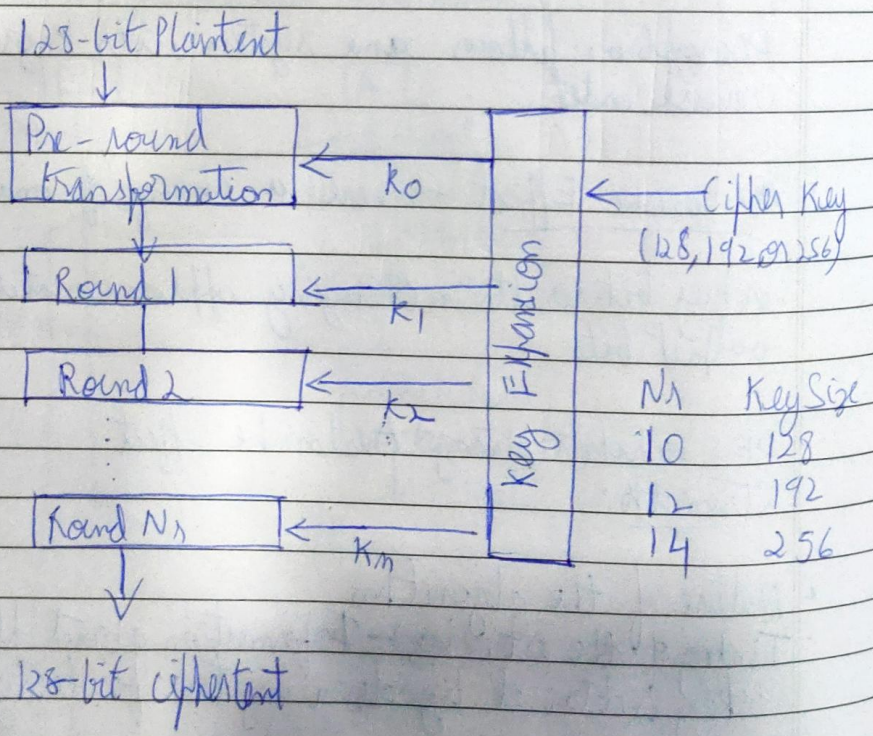
- Nature of the algorithm
- Timing of the attacks - Information about plaintext or key is obtained by observing time for decryption

Advanced Encryption Standard (AES)

- Symmetric key block cipher published by NIST

NIST - National Institute of Standards and Technology

- Non Feistel cipher encrypts block of 128 bits
- AES has 3 different versions 10, 12, 14 rounds. Each version has a different cipher key size 128, 192 or 256 but round keys are always 128 bits.



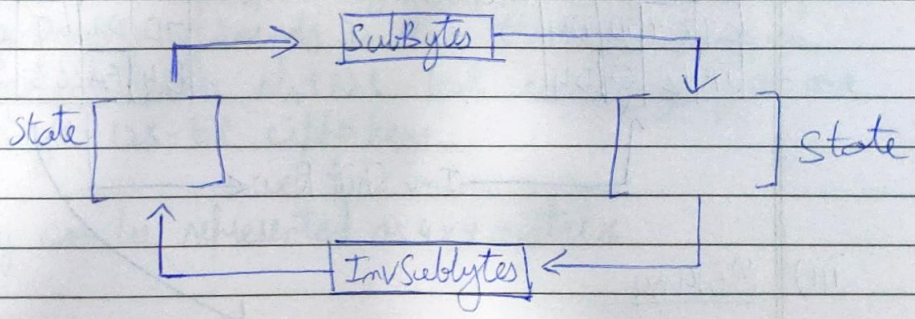
Round Contents

To provide security, AES used four types of transformation: substitution, permutation, mixing and key-adding

i) Substitution: AES uses two invertible transformation.

SubBytes: The first transformation SubBytes is used at the encryption site. To substitute a byte, we interpret the byte as two hexadecimal digits.

The SubBytes operation involves 16 independent byte-to-byte transformation



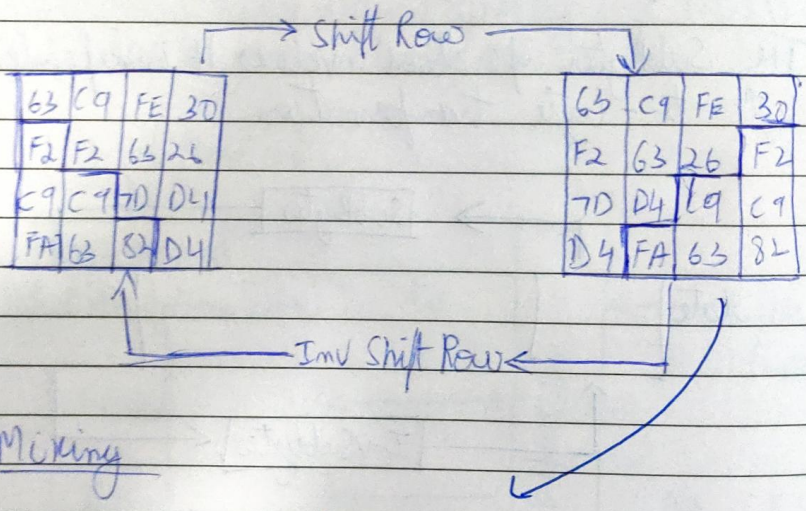
2) 128 bit message => b_0 b_1 b_2 ... b_{14} b_{15}

b_0 ... b_{12}
b_1 ... b_{13} → Sent to Rounds
b_2 ... b_{14}
b_3 ... b_{15}

ii) Shift Rows

It is another transfer found in a round which permutes the bytes

Row 0 - No Shift
1 - 1-byte shift
2 - 2-bytes shift
3 - 3-bytes shift
} Left



iii) Mixing

Column Wise Mixing of the matrix

$$\begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix} \times \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} = \text{New} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix}$$

Add operation → $\oplus$ for the multiplication
It is performed on each column

Key Adding

AddRoundKey proceeds one column at a time It adds a round key word with each state column matrix; the operation in AddRoundKey is matrix addition.

```
AddRoundKey(S) {
    for (c=0 to 3)
        Sc ← Sc ⊕ Wround+4c }
```

Key Expansion: To create round keys for each

round AES uses a key-expansion process. If the number of rounds is N_r, the key-expansion routine creates N_r+1 128-bit roundkeys from one single 128-bit cipher keys

Key can be represented as 4×4 matrix

Process:

a) $\underbrace{b_0\ b_1\ b_2\ b_3}_{W_0}\ \underbrace{\quad\quad}_{W_1}\ \cdots\ \underbrace{b_{15}}_{W_3}$

1) The first four words (W_0, W_1, W_2, W_3) are made from the cipher key is thought of as an array of 16 bytes (k_0 to k_{15}). The first four bytes (k_0 to k_3) become W_0; the next four bytes (k_4 to k_7) become W_1 and so on.

2) The rest of words (W_i for $i=4$ to 43) are made:
   i) If $(i \bmod 4) \neq 0$ $W_i = W_{i-1} \oplus W_{i-4}$
   ii) If $(i \bmod 4) = 0$, $W_i = t \oplus W_{i-4}$. Here t, a temporary

word is a result of applying ~~to~~ two ~~sets~~ routines SubWord and RotWord on w_{i-1} and XORing the result with a round constants, RCon.

$t = \text{SubWord}(\text{RotWord}(w_{i-1})) \oplus \text{RCon}_{i/4}$

Date: / /

Mathematics of Cryptography

Euclidean Algorithm

$gcd(a,0) = a$

$gcd(a,b) = gcd(b, r)$ where r is remainder of dividing a/b

★ When $gcd(a,b) = 1$ we say that a and b are relatively prime

GCD table

$gcd(2740, 1760) = 20$

$r = r_1 - q \times r_2$

q	r_1	r_2	$r \rightarrow$
1	2740	1760	980
1	1760	980	780
1	980	780	200
3	780	200	180
1	200	180	20
9	180	20	0
0	20	0	0

↳ GCD

- Extended Euclidean Algorithm is needed to find

$s \times a + t \times b = gcd(a,b)$

~~gcd(161, 28) = 7, d = -1~~

Q.) a = 161, b = 28 find s & t

$s_1 - q \times s_2$ $t_1 - q \times t_2$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
5	161	28	21	1	0	1	0	1	-5
1	28	21	7	0	1	-1	1	-5	6
3	21	7	0	1	-1	4	-5	6	-23
	(7)	0		(-1)	4		(6)	-23	

↳ gcd

s t

$7 = -1 \times 161 + 28 \times 6 = 7$

$7 = 7$

Mod division

1) 27 mod 5 = $r = 2$
2) -18 mod 14 = $r = 10$, $r_{neg} = -4$, $r + 14 = 10$
3) -7 mod 10 $\Rightarrow r_{neg} = -7$, $r_{fin} = -7 + 10 = 3$

To show congruence:

$$2 \equiv 12 \pmod{10}$$

2 integers congruent mod 10 if difference is divisible by 10.

Properties

1) $(a+b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$
2) $(a-b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$
3) $(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

Q. Find multiplicative inverse of 8 in Z_{10}.

There is no multiplicative inverse because gcd(10, 8) = 2 ≠ 1. In other words we can't find any number b/w 0 and 9 such that when multiplied by 8 result is congruent to 1

Q. Find all multiplicative inverses of in Z_{10}

Only 3 pairs : (1,1), (3,7) (9,9). The numbers 0, 2, 4, 5, 6, and 8 do not have multiplicative inverse.

$t_1 - q \times t_2$

q	r_1	r_2	r	t_1	t_2	t
1	10	8	2	0	1	-1
4	8	2	0	1	-1	5
	(2)	0		-1	5	

↳ As gcd ≠ 1 no MI

Q. Find MI of 11 in Z_{26}

q	r_1	r_2	r	t_1	t_2	t
2	26	11	4	0	1	-2
2	11	4	3	1	-2	5
1	4	3	1	-2	5	-7
3	3	1	0	5	-7	26
	(1)	0		(-7)	26	

↳ gcd = 1
So MI exists

↳ MI

Euler's Phi-Function

Euler's phi-function, $\phi(n)$, called as Euler's totient function plays a very important role in cryptography

1) $\phi(1) = 0$
2) $\phi(p) = p-1$ if p is a prime
3) $\phi(m \times n) = \phi(m) \times \phi(n)$ if m & n are relatively prime
4) $\phi(p^e) = p^e - p^{e-1}$ if p is a prime

$$n = p_1^{e_1} \times p_2^{e_2} \times \dots \times p_k^{e_k}$$

$$\phi(n) = (p_1^{e_1} - p_1^{e_1-1}) \times (p_2^{e_2} - p_2^{e_2-1}) \times \dots \times (p_k^{e_k} - p_k^{e_k-1})$$

- The difficulty of finding $\phi(n)$ depends on the difficulty of finding the factorization of n.

Q.1) $\phi(13) = 13-1 = 12$ as 13 is prime

Q.2) $\phi(10) = \phi(2) \times \phi(5) = 1 \times 4 = 4$

Q.3) ~~$\phi(15) = 13-1 = 12$~~ $\phi(240) = 2^4 \times 3^1 \times 5^1$
$\phi(240) = (2^4 - 2^3) \times (3^1 - 3^0) \times (5^1 - 5^0)$
$= 8 \times 2 \times 4 = 64$

~~Q.4)~~

Q.4) $\phi(49) = \phi(7) \times \phi(7) =$ $6 \times 6 = 36$ ✗ Not allowed as 7 & 7 must be relatively prime

$\phi(49) = 7^2 = 7^2 - 7^1 = 42$

Public Key cryptography / Assymetric key cryptography

Structure

- Algorithms are based on mathematical functions & not on bit patterns
- Use 2 separate keys

Types

1) Assymetric Keys: Two related keys a public and private key, that are used to perform complementary operations such as encryption or decryption.

2) Public Key Certificate: A digital document issued and digitally signed by the private key of a Certification Authority that binds the name of a subscriber to a public key.

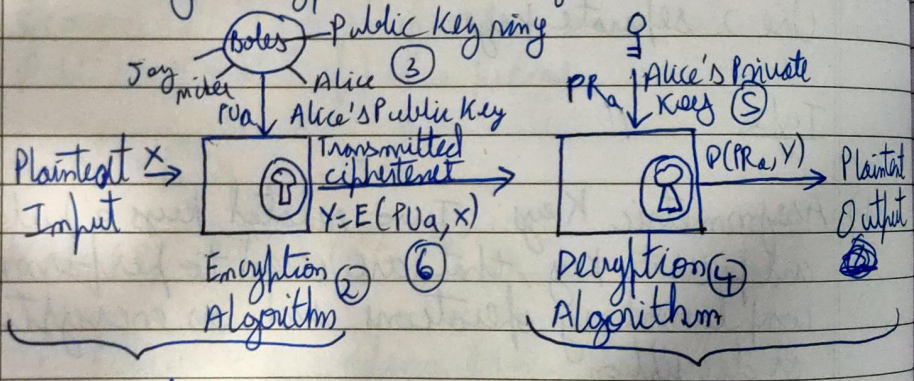
3) Public key Cryptographic Algorithm: A cryptographic algorithm that uses two related keys a public key and private key. The two keys have the property that deriving the ~~public~~ private key from public key is computationally infeasible.

4) Public Key Infrastructure: A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates, including ability to issue, maintain and revoke public key certificates.

It is computationally infeasible to determine the decryption key given only knowledge of the cryptographic algorithm and encryption key.

Either of the two related keys can be used for encryption while other is used for decryption.

Public Key Encryption has 6 ingredients



Interchange Public key ring and private to get Encryption with Private Key.

Steps:

1) Each user generates a pair of keys to be used for encryption and decryption of messages

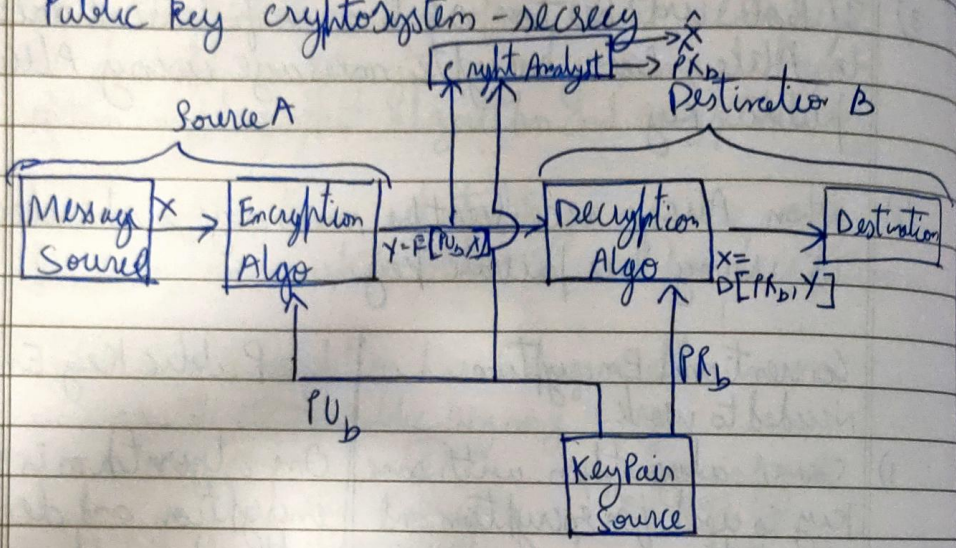
2) Each user places one of the two keys in a public register or other accessible file. The companion key is kept in private

3) If Bob wishes to send a confidential message to Alice, Bob encrypts message using Alice's public key.

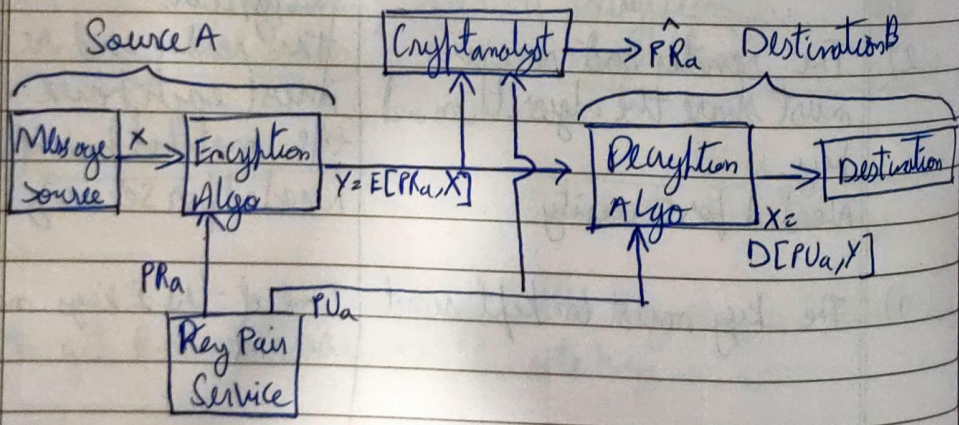
4) When Alice receives the message, she decrypts it using her private key.

Conventional Encryption Needed to work:	Public Key Encryption
1) Same algorithm with same key is used for encryption and decryption	One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption
2) The sender and receiver must share the algorithm and key.	The sender and receiver must each have one of the matched pair of keys
Needed for security:	Needed for security:
1) The key must be kept secret	One of the 2 keys must be secret
2) Impossible to decipher if no other information available	→ Same
3) Knowledge of algorithm plus samples of ciphertext must be insufficient to determine the key.	Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine key.

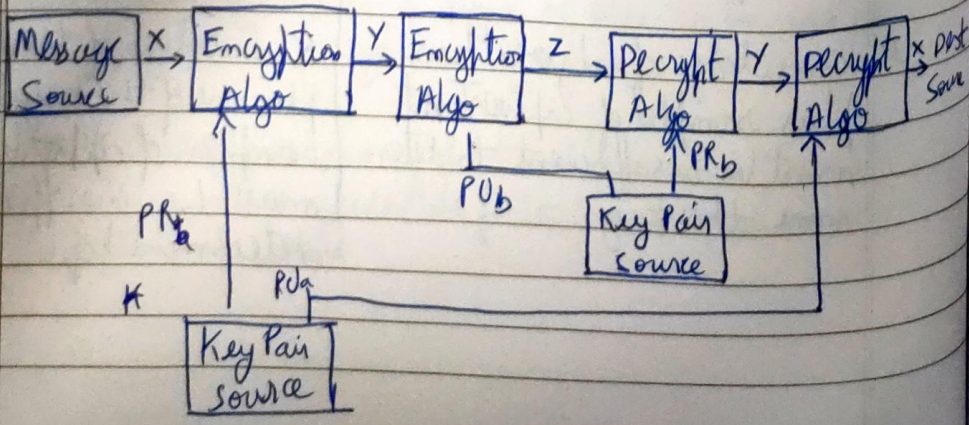
Public key cryptosystem - secrecy



Public Key Cryptosystem - Authentication



Auth and Secrecy



Applications:

1) Encryption / Decryption - Sender encrypts a message with recipient's public ~~key~~ key.

2) Digital Signature - Sender sends message with private key

3) Key Exchange - Two sides cooperate to exchange a session key.

A Cryptosystems

Algo	Encrypt/Decrypt	Digital Sign	Key Exchange
RSA	✓	✓	✓
Elliptic Curve	✓	✓	✓
Diffie-Hellman	×	×	✓
DSS	×	✓	×

Requirements of PKC

1) It is computationally easy for party B to generate a pair.

2) It is computationally easy (CE) for sender A, knowing public key and message to be encrypted

$$C = E(PU_b, M)$$

3) It is ce for receiver B to decrypt the resulting ciphertext using private key to recover original message

$$M = D(PR_b, C) = D[PR_b, E(PU_b, M)]$$

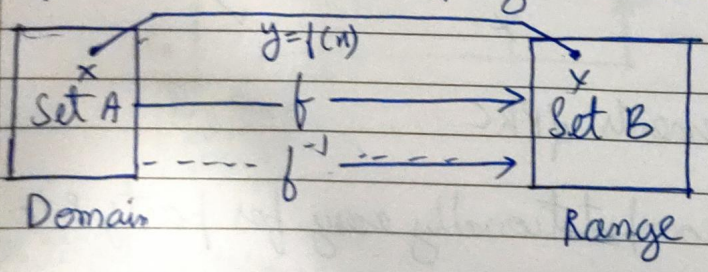
4) It is computationally infeasible for adversary knowing public key PU_b to determine private key PR_b.

5) It is CI for an adversary, knowing public key and ciphertext to recover original message

6) The two keys can be applied in either order.

Trapdoor One-Way Function

- A function as rule mapping a domain to a range



Date: / /

One way function (OWF)

- f is easy to compute
- f^{-1} is difficult to compute

Trapdoor One way function (TOWF)

- Given y and a trapdoor (secret), x can be easily computed.

Eg1: When n is large, $n = p \times q$ is a one way function. Given p and q it is always easy to calculate n, given n it is very difficult to compute p and q. This is the factorization problem.

Eg2: When n is large, the function $y = x^k \bmod n$ is a trapdoor one way function. Given x, k and n it is easy to calculate y. Given y, k and n it is very difficult to calculate x. This is the discrete logarithm problem.

Rivest, Shamir, Adleman

RSA Algorithm - Asymmetric

- Block cipher, PT and CT are integers b/w 0 to n-1 for some n.

Both sender and receiver must know value of n. The sender knows the value of e and only receiver knows d. Thus this is a public key encryption algorithm with a public key of PU = [e, n] and a private key PR = [d, n]
The requirements must be met:

1) It is possible to find values of e, d, n such that $M^{ed} \bmod n = M$ for all $M < n$
2) It is relatively easy to calculate $M^e \bmod n$ and $C^d \bmod n$ for all values of $M < n$
3) It is infeasible to determine d given e and n.

- Https is built on RSA

Key Generation

i) Select 2 large prime nos 'p' and 'q'
ii) Calculate $p \times q = n$
iii) Calculate $\phi(n) = (p-1) \times (q-1)$ // Eulers totient function
iv) Chose value of e
$1 < e < \phi(n)$ and $\gcd(\phi(n), e) = 1$ (coprime)
v) calculate

$$d \equiv e^{-1} \bmod \phi(n)$$
$$ed \equiv 1 \bmod \phi(n)$$

vi) Public key = {e, n}

vii) Private Key = {d, n}

Eg: Let p & q be 3 & 11

$n = 33$

$\phi(n) = 2 \times 10 = 20$

So let $e = 7$ as $1 < 7 < 20$, $\gcd(7, 20) = 1$

Now $d \equiv e^{-1} \bmod \phi(n)$

$de \equiv \bmod \phi(n)$

$7 \times d \equiv 1 \bmod 20$

$\downarrow$

$d = 3$

Public key = $\{7, 33\}$

Private Key = $\{3, 33\}$

Encryption $\longrightarrow$ Plaintext — As encryption using public key decryption by private key

$C = M^e \bmod n$

$C = 31^7 \bmod 33 = 4$ $\quad C = 4$

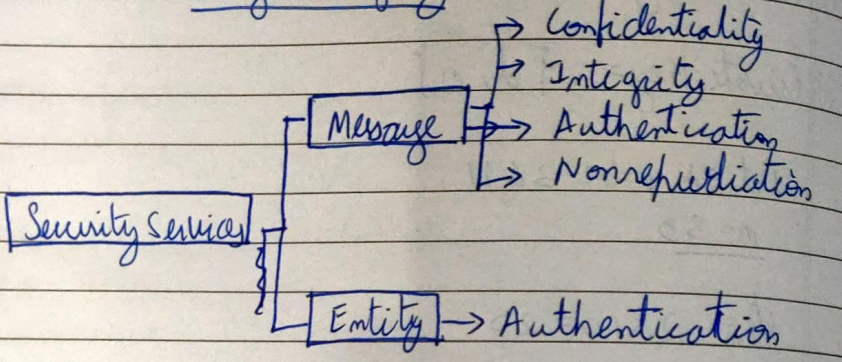
↳ Let $M = 31$

Decryption

$M = C^d \bmod n = 4^3 \bmod 33 = 31$

$M = 31$

Message Integrity



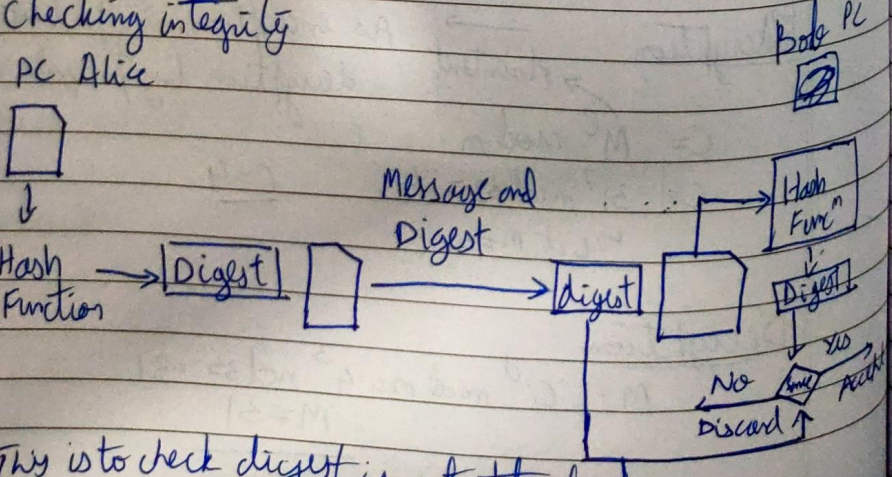
- To preserve integrity of a document both document and fingerprint are needed

Message (Document) → Hash Function (One way) → Message Digest (Fingerprint)

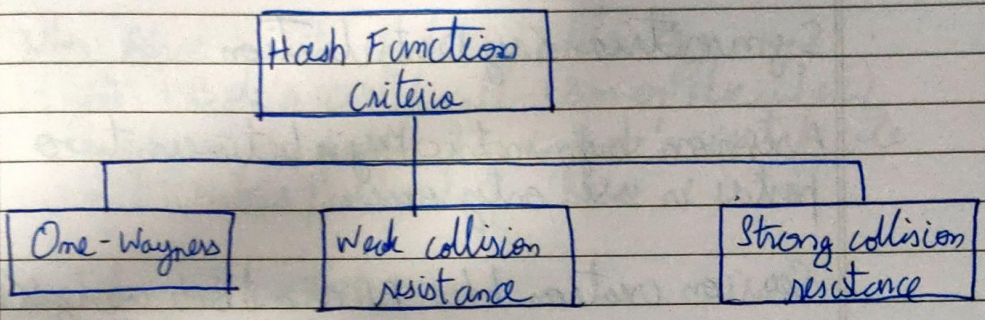
Notation
m : message
H(m) : message digest of m by using hash function H()

- The message digest needs to be kept secret or unaltered by others.

Checking integrity



This is to check digest is not attacked.



- One wayness - Cannot recover message m given its digest H(m)
- Weak collision resistance - Given message m, cannot generate another message m' such that H(m') = H(m) → ensure integrity
- Strong Collision Resistance - Sender can't generate two messages m and m' such that H(m) = H(m') ensure non repudiation.
- Divide message into multiple 512 bit blocks N bits message digest is created

★ SHA-1 has algo create N bit message digest out of message of 512 bit blocks. SHA-1 has message digest of 160 bits

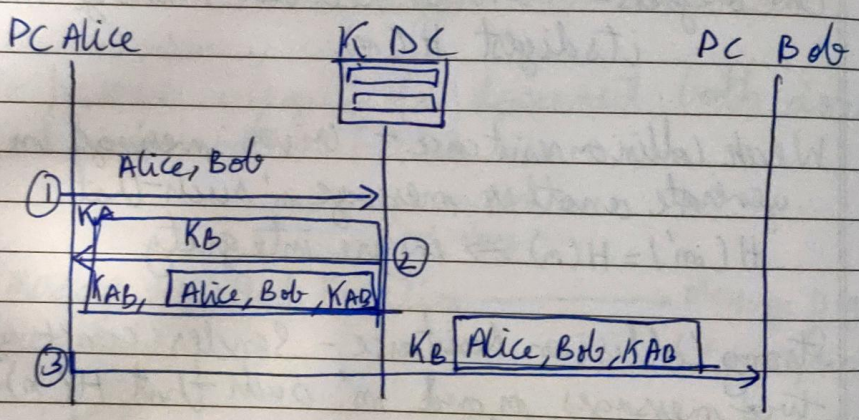
★ MD5 - popular hash algorithm. It is older generation than SHA-1.

Key Management

Symmetric Key Distribution

A session symmetric key is between two parties is used only once.

Session creation b/w Alice and Bob using KDC



In public key cryptography everyone has access to everyone's public key.

Checking if obtained public key is actually receiver's

Certification Authority (CA): binds public key to particular entity, E.

E (person, router) registers its public key with CA.
- E provides proof of identity to CA
- CA creates certificate binding E to its public key
- Certificate containing E's public key digitally signed by CA.

When Alice wants Bob's public key
- gets Bob's certificate (Bob or elsewhere)
- Apply CA's public key to Bob's certificate get Bob's public key.

Certificate contents:

Serial number (unique to issuer)
info about certificate owner, including algorithm and key value itself.

Digital Signature

It is used to check authenticity of the sender.

It needs a public-key system
Notations
m: message
H(m): message digest
K_A^- : Private key of user A
K_A^+ : Public key of user A
K_{AB} : Symmetric key b/w A & B
K(m)

Case 1: Signing message itself in digital signature
Private key for encryption and public key for decryption

- It provides no confidentiality (message isn't secret)

Case 2: For message confidentiality, we use the private and public keys of the receiver.

Digital signature provides 3/5 services for security systems:

i) Integrity
ii) Authentication
iii) Non-repudiation

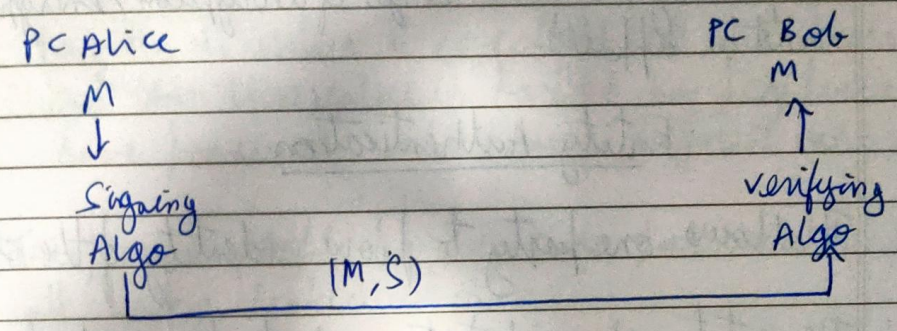
- A conventional signature is included in the document but when we sign the document digitally we send the signature as a separate document.

- Verification - For conventional signature the recipient compares the signature on document with signature on file. For digital signature. The recipient needs to apply a verification technique to combination of message and signature to verify the authenticity.

- Relationship - Conventional sign one to many documents Digital sign, one-to-one ~~Sign~~ b/w signature and a message.

- Duplicity - Copy of signed document can be distinguished from original one on file. In digital there is no such distinction unless there is a factor of time

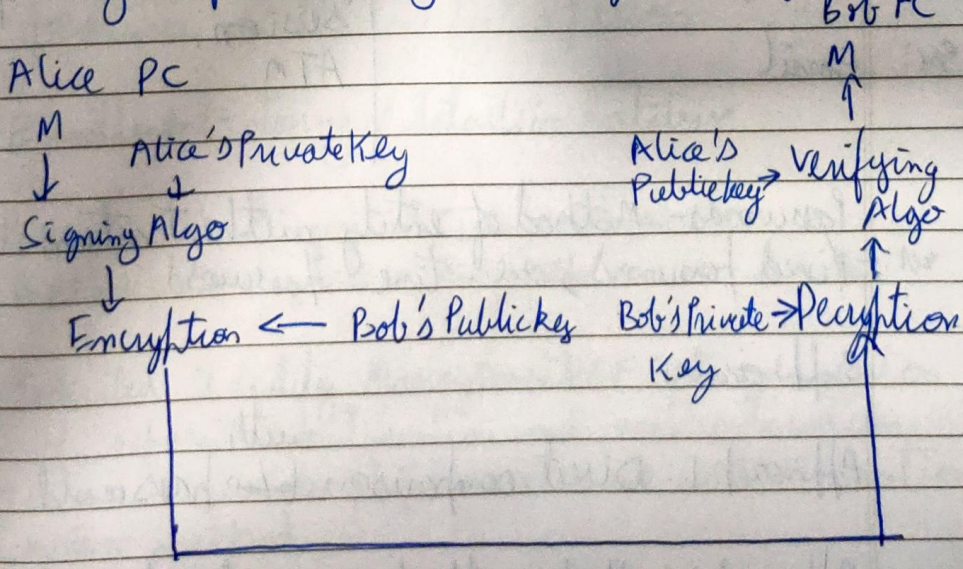
Digital Signature Process



Digital Signature needs public-key system

- Digital signature provides message authentication
- Digital Signature provides message integrity
- Non repudiation can be provided using a trusted party

Adding confidentiality to a digital signature



- Digital Signature doesn't provide privacy. For privacy, another layer of decryption / encryption must be applied.

Entity Authentication

- It allows one party to prove identity of the other
- The entity whose identity needs to be verified is called claimant
- * Party proving identity is called verifier.

Message Auth	Entity Auth
Not in Real time	In Real time
Needs to be done for each message	Authenticates claimant for entire duration of a session.
eg: Email	ATM

eg: Passwords - Method of entity authentication
Fixed password, one-time password.

3 approaches:

Approach 1: Direct comparison with password

Approach 2: Hashing the password and comparison with hashed value

Approach 3: Salting the password

12 bit salt value is concatenated with password and then this value is hashed so people with same passwords will have a different hash value.

- This prevents people having same passwords from all being leaked at once.

Dictionary Attack: create a list of numbers apply hash function.

Approach 4: 2 identification techniques are combined.

Ex: Use of ATM card with Pin.

Biometrics

- Measurement of physiological or behavioral features that identify a person.

- Enrollment - storing of details in database

Physiological - Fingerprint, Iris, retinal etc
Behavioral - signature, Keystroke

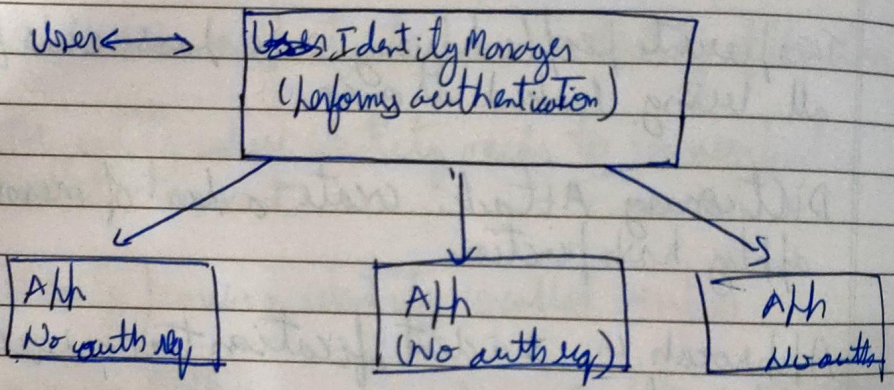
Federated Identity Management (FIM) is a union of separate identification and authentication

- It maintains one profile with one authentication ~~system~~ method.

Ex: Oauth, OpenID

When two domains are federated, a user can authenticate to one domain and access resources in the other domain without having to perform a separate login process.

FIM



The key difference b/w Single Sign on Shell (SSO) and FIM is that SSO is designed to authenticate a single credential across various systems within one organization, FIM offers single access to multiple apps.

Access Control: Limits who can access what in what ways.

Access Policie: They are a list of roles and the resources with which roles are to be provisioned or deprovisioned.

Effective access implementation:

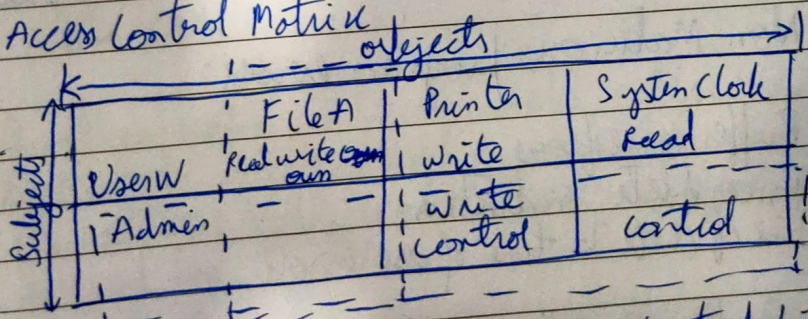
1) Check every access
2) Enforce least privileges - Give bare minimum access
3) Verify acceptable usage - check activity performed on an object is appropriate

Implementing Access Control: by OS

Difficulties:

1) List is too big if many shared objects, deletion must be reflected in all directories.
2) Propagation of access rights: serious problem in networks
3) Pseudonyms: File F may exist from multiple subjects.

Access Control Matrix



↳ ACL -> Access Control List
↳ shows all subjects access to an object.

Privilege List: Privilege or access rights for a subject

Programming Insights

Challenges to Writing Secure Code:

- Size and complexity of code is a challenge
- Size alone increases number of possible points of vulnerability
- Interaction of multiple pieces leads to many more possible vulnerabilities
- Specifications are focused on functional requirements.
- It is essentially impossible to list and test all of the things that code should not allow.

Non Malicious Program errors:

1) Buffer overflows
2) Incomplete mediation
3) Time of check to time of use errors

Buffer Overflows

- Failure to check for excessive data

Cases to consider:

1) The array/buffer is in user space
2) The out of bounds access only steps on user space.
3) It may or may not trash user data
4) ~~The 10th post~~ The O/S should kill the process for violating memory restrictions.
5) No natural boundary on what user might submit into the buffer.

Attack 1: On the system code

- Given knowledge of relative position of the buffer and system code in memory.
- The buffer is overflowed to replace valid system code with something else.
- A primitive attack would just kill the system code.

- A sophisticated attack would replace valid system code with altered system code.
- The altered code could have any effect as desired by attacker.

- Game over - the attacker has just succeeded in completely hijacking the system.

Attack 2: On the Stack

- Given knowledge of relative position of buffer and the system Stack.
- Buffer is overflowed to replace valid values in stack with something else
- A more sophisticated attack would change either calling address or return address.
- False code would be loaded this makes it possible to run false code under system privileges.

Overflow Countermeasures

- Check length before writing
- Confirm that array subscripts are within limits
- Double check boundary condition code.
- Monitor ~~and~~ input and accept only as many characters as can be handled
- Check procedure that might overrun their space.

Incomplete Mediation

- It means that data is exposed somewhere in the pathway b/w submission and acceptance.

Eg: Browser ~~takes~~ takes in date and phone number which is forwarded to server as an URL.

Validate All Inputs

Input values may have given by a choice list.

- Values may have been tested for a valid range

Time of check – Time of Use Errors

- Between access check and use data must be protected

Counter Measures

- Access checking software must own request data until request action is completed.
- Malicious Software – Program planted by an agent with malicious intent to cause unanticipated effects
- Virus – code with malicious purpose and intended to spread.
- Transient virus – Life time depends on life of host program
- Resident virus – locates in memory, remains active or be activated as a stand alone program

Intrusive

Worms - This is a program that, copies of itself through a network.

Worms spread copies of itself as a stand alone program.

Bot is a kind of worm used invast numbers by search engines.

Trojan Horse - Program with benign apparent effect but second, hidden malicious effect.

Counter Measures for developers:

1) modularity - System design limits the damage any fault causes.

2) Mutual suspicion - They operate as if other routines in the System were malicious or incorrect.

3) Confinement - Technique used by an OS on a suspected program to help ensure that possible damage doesn't spread to other parts of a system.

A confined program is strictly limited in what System resources it can access.

4) Simplicity - Less room for error.

Penetration testing for security - Involves the team of experts trying to crack the system being tested.

- The artistic side requires careful analysis and creativity in choosing the best course. Scientific side requires rigor, order, precision and organization.

Steps in Hacking:

1) Reconnaissance - Foot printing, Collecting information
2) Scanning - Scanning for open ports
3) Gaining Access - To Reach into a system
4) Maintaining Access
5) Clearing Tracks

Phishing

- Practice of sending fraudulent communications that appear to come from a reputable source

Types of Phishing:

- Spear Phishing
- Whaling
- Smishing
- Vishing

- Brute Force Attacks (Exhaustive search) – Process to carry out a string of continuous attempts to get information required.
- DOS and DDOS – Overwhelms a system's resources so that it cannot respond to service requests.
- Session Hijacking (Man in the middle) – Attacker hijacks a session b/w trusted client and network server.
- Botnets are the millions of systems infected with malware under hacker control in order to carry DDOS. Difficult to trace because botnets in different geographic location.
- Mitigation – RFC 3704 filtering which will deny traffic from spoofed addresses ensure traffic is traceable.
- Black hole filtering – Drops undesireable traffic before it enters a protected network.