6. CRYPTOGRAPHY & SYMMETRIC KEY ALGORITHMS

CRYPTOGRAPHY GOALS
- confidentiality
- Authentication
- Nonrepudiation
- Integrity

(P.T.O.)

Of sensitive information AT Rest, In transit, In use

HISTORY

Caesar cipher

A → D
B → E
} ROT3

↳ Vulnerable to frequency analysis attack

Note

↳ If you can decode using Frequency Analysis, then it's transposition cipher.

↳ Substitution cipher are more prone to Periodic Analysis

Examination of frequency based on repeated use of key

1. Confidentiality —— what it means?

Data remains private in 3 situations:

- At Rest
- In Transit or Data in use
- In use

To enforce confidentiality → 2 Types of Cryptosystems

- Symmetric Cryptosystem → shared key
- Asymmetric Cryptosystem → private & Public key

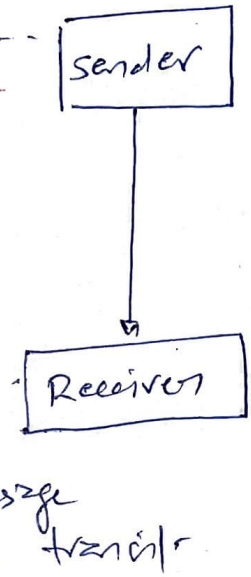
Think different kinds of Data with Attacks.

- Data At Rest — theft or loss of physical device
- Data in Transit — Eavesdropping
- Data in use — Unauthorized Access

2. Integrity ——— what it means?

Data is not altered from the time it was created and the time it was accessed.

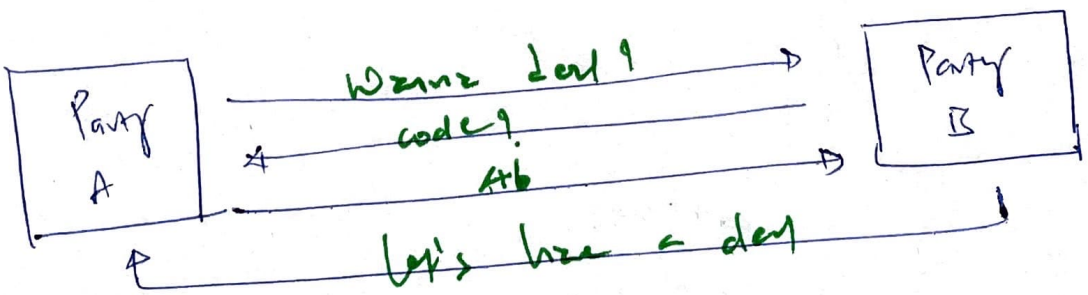
To enforce integrity → Digital signature



→ Ensures message wasn't altered in transit

3. Authentication ——— what it means?

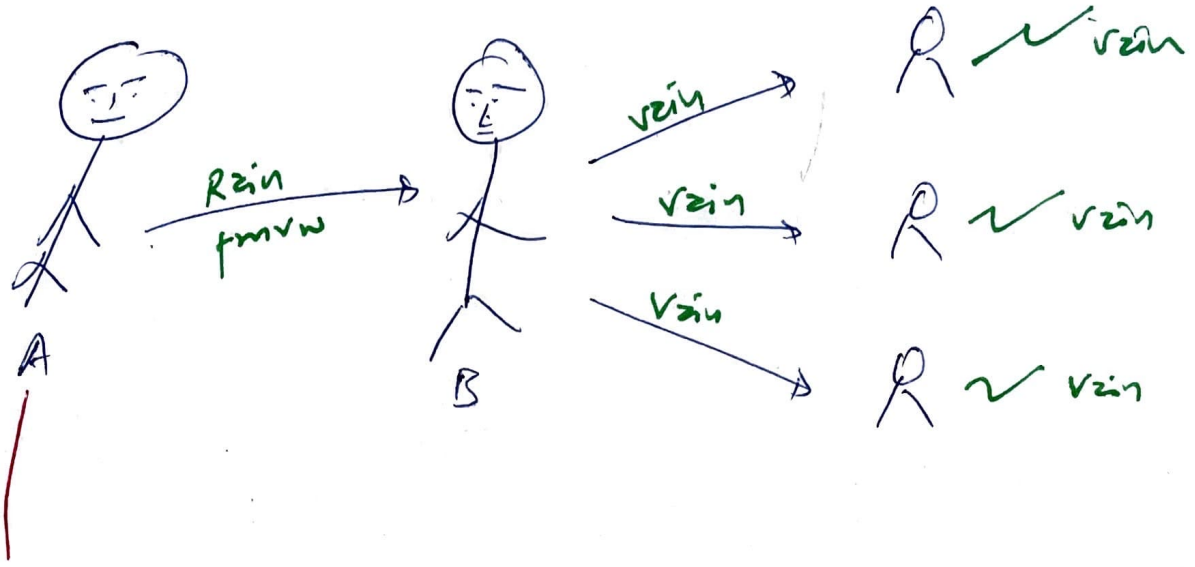
To make sure person is genine what he meant to be



→ Both party have a secret code to establish secure comm

→ Uses challenge-response authentication technique.

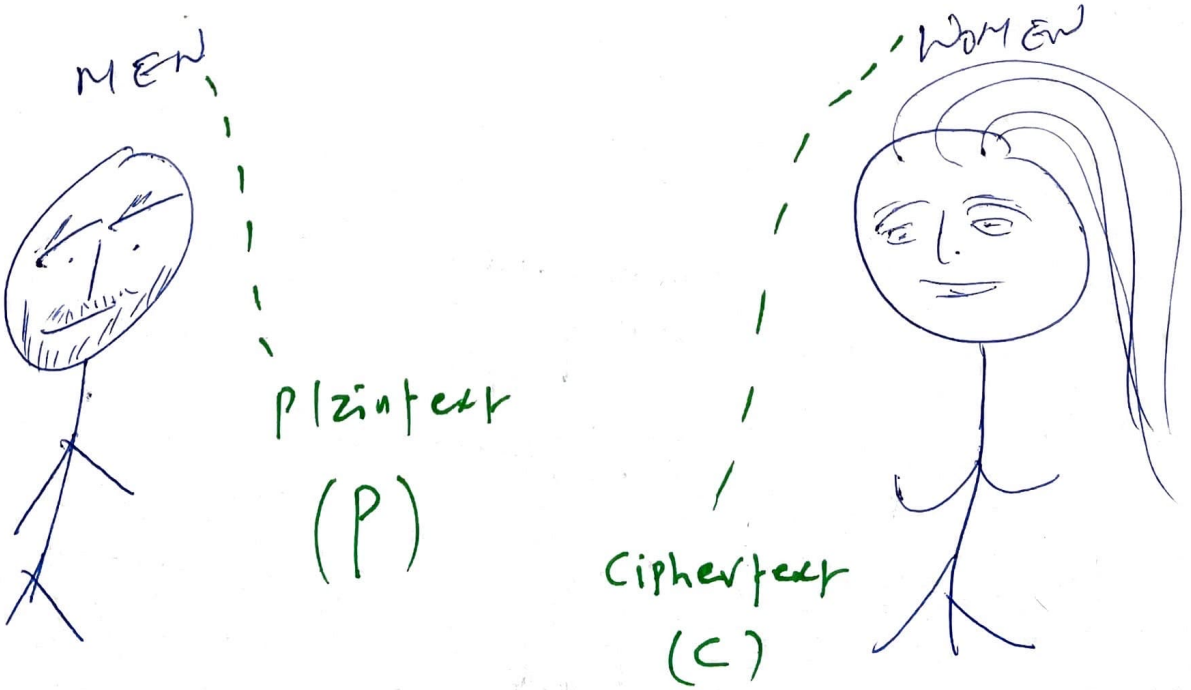
4. Nonrepudiation



Hey! Got I didn't tell that.

↳ Symmetric key ≠ Non repudiation (Authenticity)

↳ Asymmetric key = Non repudiation



Cryptographic Algorithms $\propto$ KEYS = To maintain SECURITY

Secret Key

Private

Open to Public except crypto keys

= The Enemy Knows the system. (Kerckhoff's Principle)

CRYPTOGRAPHY CONCEPTS

AND

X	Y	X ^ Y
0	0	0
0	1	0
1	0	0
1	1	1

OR

X	Y	X v Y
0	0	0
0	1	1
1	0	1
1	1	1

NOT

X	¬X
0	1
1	0

EX OR

X	Y	X ⊕ Y
0	0	0
0	1	1
1	0	1
1	1	0

Modulo Function

8 mod 2 = 0

15 mod 3 = 0

10 mod 3 = 1

33 mod 8 = 1

6 mod 8 = 2

6 mod 8 =

One-way Functions

- Produce large prime numbers as output
So finding input value becomes IMPOSSIBLE!

Nonce

(number used only once)

- Example of Nonce is IV – initialization vector
- IV is random string XORed with message

core IV concept

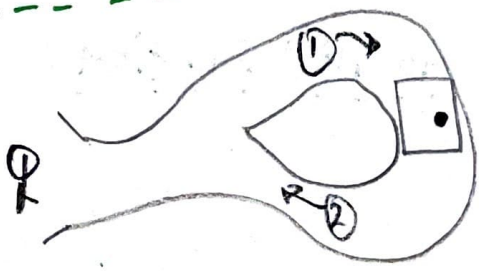
Salt

if IV is not used, then two identical plaintext that are encrypted with same key will create same cipher text. Algorithm use IV & key to provide randomness in Encryption process.

- IV creates unique cipher text even if same message is encrypted using same key.

Zero-Knowledge Proof

Prove knowledge of X to 3rd party without revealing secret / key



Split Knowledge

↳ M of N control (M<=N)

↳ E.g Key Escrow Database

Seperation of Duties

An estimation how long attacker will take to break a cryptosystem

(work factor)

P.t.o — Work Function

Strength of crypto system = cost & time of work function

$100K

$100K work of cryptography solution

Remember ... Work function > Attack value

CRYPTOGRAPHY CONCEPTS (contd ...) → CIPHER

↳ Meant to hide true meaning of message

Don't confuse with

CODE

↳ Not all codes are secret

↳ "Eagle has landed" to report arrival of Enemy crypt

This can convey confidential message but may not achieve confidentiality

difference:

↳ Achieves confidentiality with variety of techniques.

↳ codes work on words and phrases while ciphers works on individual characters and bits.

1. Transposition cipher - scramble

↳ scrambling / rearranging letters of plaintext ⇒ ciphertext

↳ can use "columnar transpotion" for more complexity

Block cipher

2. Substitution Cipher

↳ Roll caesar cipher (ROT3)

↳ Uses encryption algorithm to replace characters of plaintext with other characters.

↳ Polyalphabetic : Another substitution cipher

- Protects against direct frequency analysis but vulnerable to Periodic analysis.

3. One-time Pads — The only perfect Cryptosystem

↳ Vernam cipher

↳ The key length is as long as message!

↳ impossible to break when used correctly

- need physical protection
- one time pads must be randomly generated values
- one pad = one time use
- long keys = difficult to distribute
- Securely distributed to its destination

VENONA

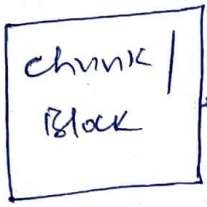
Entire soviet union project was declassified as one-time pad ~~decrypto~~ generated receiving key instead of random one.

4. Running Key cipher

↳ Book cipher ——— MOBY DICK
↳ page 46
↳ 3rd para

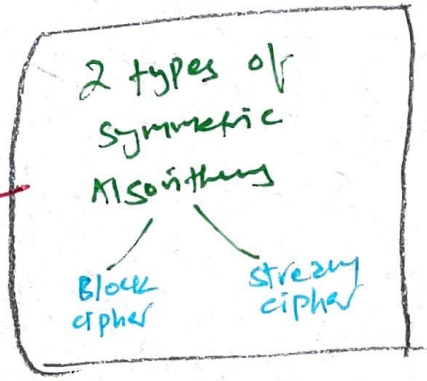
↳ Unlike one time pad which requires physical exchange of pads, two parties need a common book.

5. Block Cipher



↳ Transposition as example of block cipher + many modern encryption algorithm.

p.t.o End 10,000 ft.



6. Stream Ciphers

↳ one character at a time ← ceesar / one time pad

↳ Even Block cipher but buffer fills all data & process one at a time

---

Cryptographic algorithm's 2 basic operation to obscure plaintext message

Confusion — Attackers can't determine plaintext - Attacker can't determine changes relationship b/w ciphertext & plaintext resulting ciphertext to determine key.

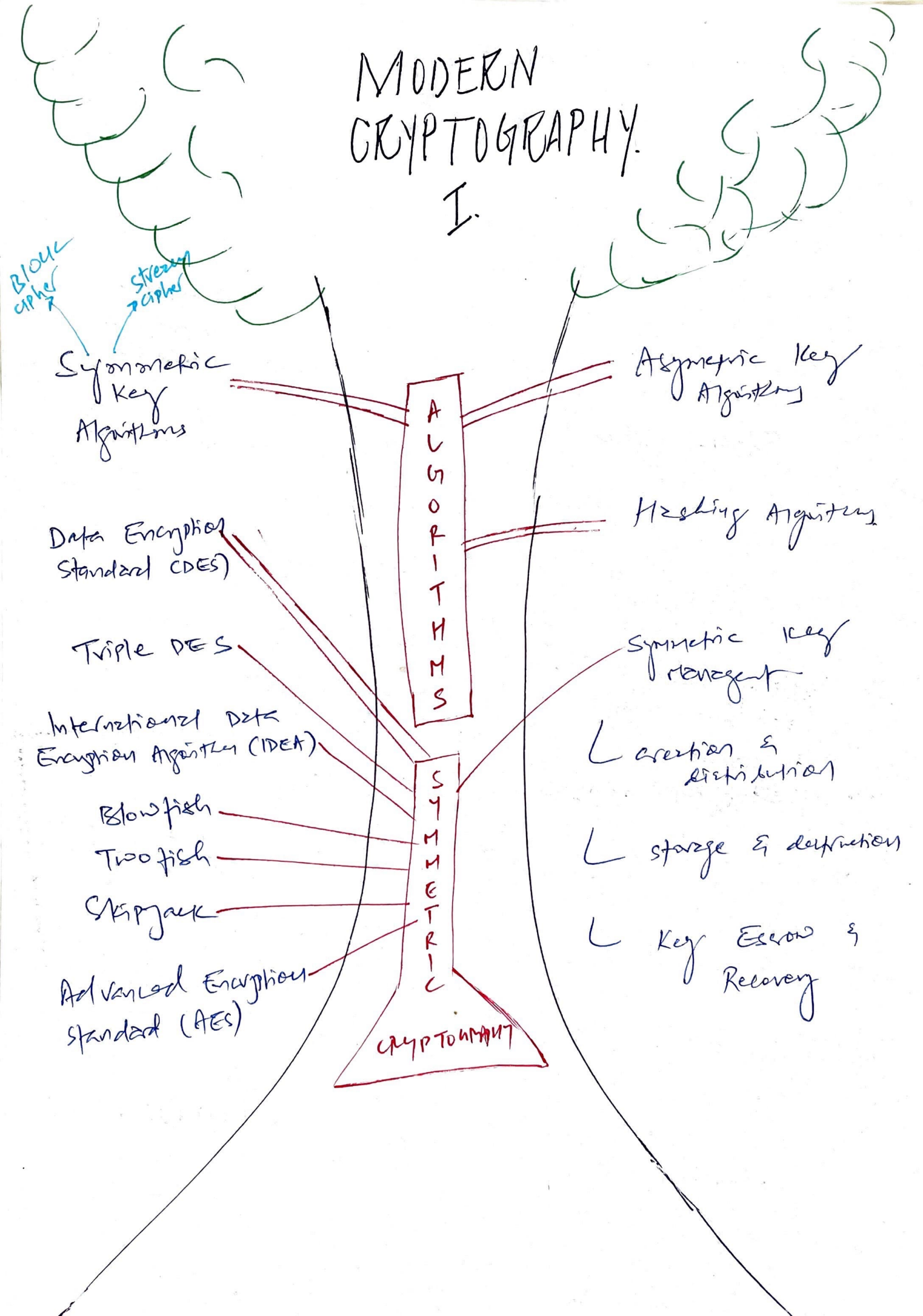
p.t.o End

↳ better clarity

Diffusion — change in plaintext results in multiple changes through the ciphertext

MODERN CRYPTOGRAPHY

I.



Cryptography perspective

THEN

Algorithm + secret key

↑ Hide from public

"Security through obscurity"

NOW

Algorithm

Secret keys — secret

Available to public = improves security

Cryptographic keys

the length of the key directly relates to work function of the cryptosystem.

longer = secure

3 types of Algorithms

- Symmetric Encryption
- Asymmetric Encryption
- Hashing

1. Symmetric key Algorithm.

↳ private key cryptography

- Not to confused with private - public key pair.
- Private key means two people share same secret (to encrypt & decrypt message).

↳ Problem with Symmetric Key Cryptography

- * No non-repudiation but provides Confidentiality
- Key distribution = problem → QKD: one of Quantum Key Distribution will solve this problem
- Not scalable
- Frequent key generation

HOW MANY KEYS?

$\frac{100\ (99)}{2} = \frac{9900}{2} = 4950$

$\frac{n(n-1)}{2}$

n = parties

- It's fast.

strength ..... weakness

2. Asymmetric Key Algorithms ---- ch:7

best pair

- Sender Encrypt message with Receiver's public key
- Receiver Decrypt message with it's own private key.

- once sender encrypt, he/she/they can't decrypt it with their private key

HOW MANY KEYS?

↳ DOUBLE IT

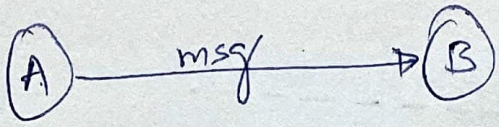
2 → 4
5 → 10
10 → 20
100 → 200

- Web server decrypt with it's private key

That's what happen when we browse web site (OSCP P257)

- Browser gets web server's Public key, browser generates Symmetric key & encrypt with web server's public key

↳ Asymmetric key algorithm = support for Digital Signature



How B verify that msg came from A?

1. A ~~Creates~~ creates message digest with hashing algorithm
2. A Encrypt msg with own private key
3. B decrypt msg with A's public key.

↳ Asymmetric strengths

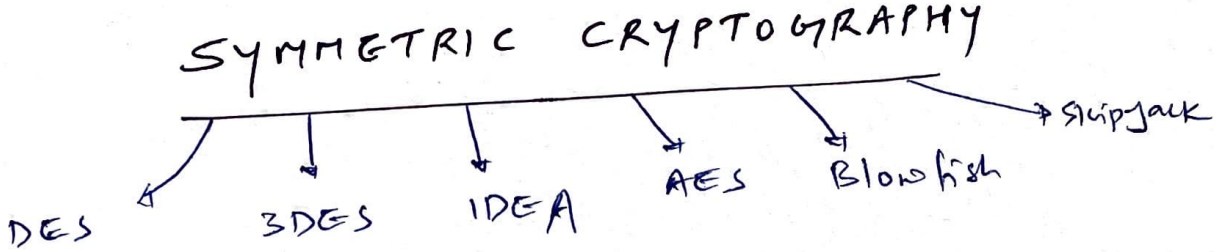
- Every new user = one pair of public-private key
- Generate only key if Private key is compromised
- Easy key revocation / removing user from system
* - Provides nonrepudiation, integrity & confidentiality, authentication
- Easy key distribution process = make your public key available on internet.
* - No preexisting communication link needs to exist = Batman vs Joker can be friends
* - scalable

↳ Asymmetric weakness = slow

3. Hashing Algorithms --- Ch: 7

↳ Recall MESSAGE DIGEST as part of Digital signature support from Asymmetric Key Algorithm.

Hash algorithm produces MD.



* Data Encryption Standard (DES)

- Insecure, but still a building block of 3DES
- ~~does~~ 64-bit block cipher for all five modes of operation techniques
- Uses 56-bit Key to drive encryption & Decryption process.

Remaining 8-bits are used for detecting tampering or corruption of the key.

→ all 64-bit block

5 modes for DES operation:

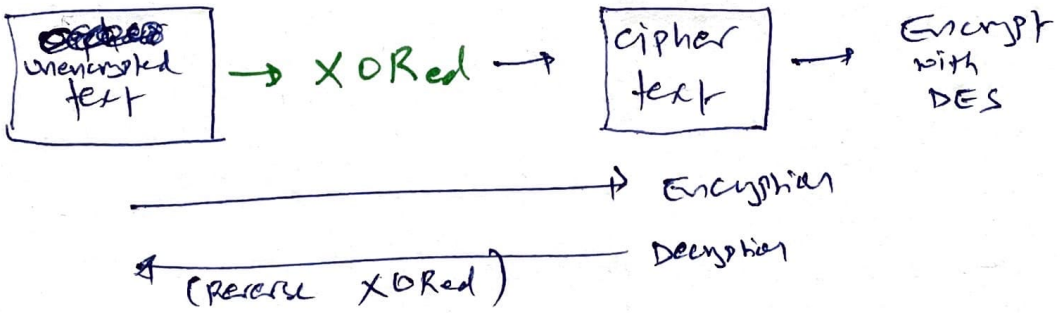
i) ECB - Electronic code Book

- Encrypts the block with chosen key. If algorithm encounters same block, it produces same encrypted block.

Using same key + lock for all the doors → least secure

- Used to exchange small amount of data.

ii) CBC - Cipher Block chaining



- Implements IV & XOR: produces unique output everytime operation is performed

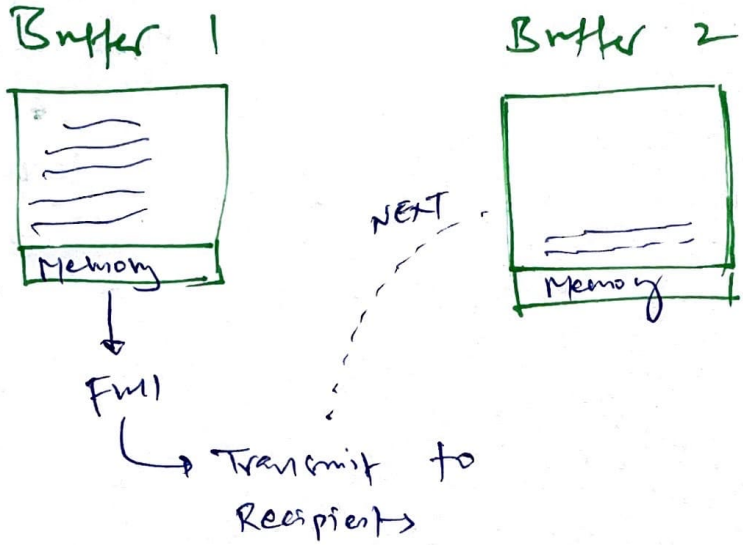
* If Block is corrupted during transmission, it's impossible to decrypt that block & following blocks.

chaining

Output Feedback Mode solves this problem

iii) Cipher Feedback - CFB

- Stream version of CBC, uses XOR
- Instead of blocks, it uses memory buffers
- It uses IV and chaining.



iv) Output feedback - OFB

- Similar to CFB, instead of XORing encrypted version of previous block of cipher text, DES XORs plaintext with seed value

* Advantage: No chain vexation like transmission error in CBC

v) Counter Mode - CTR

- ideal for parallel computing as it allows encryption & decryption into multiple independent steps.
- Use stream cipher similar to CFB. Instead of creating seed value for Enc/Dec. operation, it simply use counter increments for each operation.

* Triple DES (3DES)

- Because DES' 56-bit key length was insecure.

4 versions

1 DES-EEE3

Plaintext × three-times Encryption with different keys

K1 K2 K3

$E(P, K)$ — Encryption; P: Plaintext; K: key

$$E(K_1, E(K_2, E(K_3, P)))$$

Effective key lc = 168 bits

After Attack KL = 112 bits.

2 DES-EDE3

- Same as 1 but replace second encryption operation with decryption

$$E(K_1, D(K_2, E(K_3, P)))$$

KL = 112-bits

only uses two keys

3 DES-EEE2

4 DES-EDE2

Effective KL = 112-bit

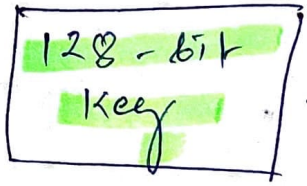
After Attack KL = 80-bit

$$E(K_1, D(K_2, E(K_1, P)))$$

$$E(K_1, E(K_2, E(K_1, P)))$$

* International Data Encryption Algorithm (IDEA)

- Developed to respond insufficient KL in DES
- Like DES, it uses 64-bit cipher block of plaintext / ciphertext
- Unlik DES' 56-bit KL, IDEA use 128-bit KL.
- IDEA capable of using all 5 modes of DES operation



— broken up into a series of operation into 52 16-bit subkeys

- IDEA implementation: Pretty Good privacy (PGP) for secure email package.

* Blowfish —more secure→ Twofish

- Bruce Schneie's alternative to DES & IDES
- 64-bit block } fast
- KL range: 32-bit to 448-bit

- 128-bit block
- KL: 256-bit
- 2 techniques
  - Pre-whitening
  - Post-whitening

* Skipjack

- 64-bit block & key
- KL: 80-bit
- Supports DES's 5 operation modes
- Embraced by US Government

Not embraced by cryptographic community due to mistrust of Escrow procedures within US Government.

TWIST

Supports ESCROW of Encryption keys.

* RC5 (Rivest cipher)

- From people who developed RSA Asymmetric Algorithm
- Block size: 32, 64 or 128 bits
- KL: 0 to 2048 bits

* AES - Advanced Encryption Standard

- 2000: Nist announced AES / Rijndael
- KL: 128-bits, 192-bits, 256-bits
  - 128-bits: 10 rounds of Encryption
  - 192-bits: 12 rounds
  - 256-bits: 14 rounds
- Only allows 128-bit blocks

* Skipjack

- 64-bit block size
- KL: 80-bit
- Supports DES's operation modes
- Embraced by US Government

Not embraced by cryptographic community due to mistrust of Escrow procedures within US Government.

TWIST

Supports ESCROW of Encryption keys.

* RC5 (Rivest cipher)

- From People who developed RSA Asymmetric Algorithm
- Block size: 32, 64 or 128 bits
- KL: 0 to 2048 bits

* AES - Advanced Encryption standard

- 2000: Nist enhanced AES / Rijndael
- KL: 128-bits, 192-bits, 256-bits
  - 128-bits: 10 rounds of Encryption
  - 192-bits: 12 rounds
  - 256-bits: 14 rounds
- Only allows 128-bit blocks

याद रखने - Symmetric Memorization chart

Name	Block size	Key size
Data Encrypt. Standard (DES)	64-bit block cipher	56 bits
3DES	64	112 or 168
IDEA (used in PGP) - uses DES's 5 modes	64	128
Blowfish — uses variable key strength	64	32 - 448
Twofish (Pre-whitening, Post whitening)	128	1-256
AES	128	128, 192, 256 (10) (12) (14)
Skipjack	64	80
Rijndael	variable	128, 192, 168
Rivest cipher 2 (RC2)	64	128
Rivest cipher 5 (RC5)	32, 64, 128	~~0 - 2040~~ 0 - 2040

SYMMETRIC KEY MANAGEMENT

Creation & Distribution of symmetric key

- Diffie-Hellman - Page 227
- Public Key Encryption
  - IPSec
- Secure-RPC (S-RPC) employs Diffie-Hellman for key exchange.
- Offline Distribution (out-of-band method)
  - ♥ love letter in her hand

Storage & Destruction of sym. keys

- Vault
- Principle of Split Knowledge
- Consider Key rotation
- Never store Encryption key where Encrypted Data resides

Key Escrow & Recovery

- When Government wanted to obtain cryptographic key under court order

2 APPROACHES

Escrowed Encryption Standard

- idea behind skipjack
- technology is available but likely to happen where Government can decrypt the ciphertext.

Fair Cryptosystem

- Secret key divided into 2 or more pieces & given to independent 3rd parties

To Enforce confidentiality

Symmetric → shared key

Asymmetric → Private | public key

To Enforce Integrity

Digital signature

To Enforce Authentication

challenge-response technique

To Enforce Nonrepudiation

Seperation of Duty

Split knowledge → M<=N → of key escrow database

3 of 8 required to launch Nuclear attack

- min 3 person required out of 8
- 3(M) is less than N(8)

Codes —— words & phrases

ciphers —— bits & characters

Block cipher → Transposition

stream cipher → ceaser

stream cipher → one-time pad → key is as long as the message

Book cipher → running key → key is as long as the message

Cryptographic Algorithm's two operations

CONFUSION

DIFFUSION

- confusion makes relationship b/w plaintext & keys complicated
- Diffusion → plaintext has influence over ciphertext.
- Diffusion occurs when change in plaintext results multiple changes throughout in ciphertext.

Symmetric → Confidentiality.

Asymmetric → Confidentiality, Nonrepudiation, Authentication, Integrity

Why Symmetric Encryption ≠ Nonrepudiation

Any communication party can Encrypt and Decrypt message with shared key, there is no way to know where message is originated from.

Domain correlation example