Cryptographic Basics

07 February 2024 15:51

1) Asy and Sym encryptions - 5) Hashing.
2) DS - Digital Signatures
3) Certificates
4) CA
6) Algorithms - Crypto
- DES, AES, 3-DES, RSA, SHA 256, El-gamal, Elliptic ECC

What is symmetric encryption?

- Using one shared Secret to encrypt the data/Message.
- Sym: K, M - Message / Plaintext
C - cipher text
E - Encryption algorithm $E_K(M) = C$

$$C = E(M|K) \equiv E_K(M) \equiv C \equiv D_K(C) \equiv M$$
$$D_K(C) = M$$

Public key cryptography

2 keys - Public key - Publicly available - can be used by any one
- Private key - Only owned by the user/owner.

(PU_K, Pr_K) - Pair of Keys - Not publicly available.
- Encrypt with any key - Decrypt with any key
- You need both the keys to encrypt/decrypt the message

To achieve confidentiality - PKC

M - No one should be able to decrypt your message other than the recipient

Bob: $M - A(PU_K)$ → Alice: $M - A(PU_K) - A(Pr_K)$ → M

$B(PU_K)$ $B(Pr_K)$

No one in the middle - will be able to decrypt the message. $A(PU_K)$ $A(Pr_K)$

Pu - Pr: Lock and key.

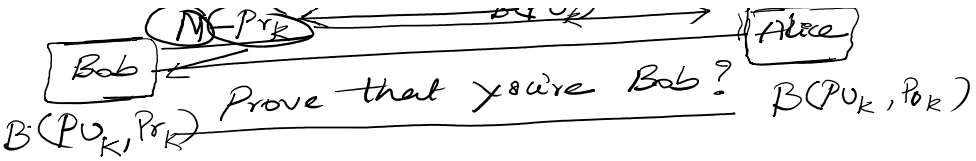
1) The Sender encrypts the message with the recipients public key - only the recipient will be able to decrypt the message using his/her private key.

How to achieve ~~integrity~~ using PKC -

Authentication Authentication

Bob: $M - Pr_K$ → $B(PU_K)$ → Alice

Bob: Prove that you're Bob? $B(PU_K, Pr_K)$



D) The Sender encrypts the message with his/her private key. The recipient will decrypt the message using the sender's public key. This authenticates the sender because only the sender could have sent the message as the private key is only known by the Sender.

↓

This is the concept behind — Digital signature

Digital signature — {Authenticity, Integrity}

— confidentiality ✗

Symmetric — Encryption algorithms : Digital signature

Mode of operation — Veena

Explain? — DSA

Block ciphers — Digital signature

Message M — Non-Repudiation — Algorithms

Non-Repudiation — Produce a digital signature

Email / File / Message — Bob — ?

If I send a message — Veena — original sender

later — I can't deny I have — Modified

— {Non-Repudiation} — How is it achieved — sent the message

Message

M — Hash — M|H

Cyber security — Attacks against cyber

Info-security — protecting your information

Pr — CIA

M|E(H)

Cyber devices

TLS — Attacks

Info Sec — Infosec

Data at rest

Validation of digital signature — {Digital Sig Alg — DSA — NIST}

$D_{Pu}(E_{Pr}(H)) = H$

(Hybrid signature)

$D_{Pu}(E_{Pr}(H)) \equiv H$

Infosec

$\#(M) \equiv H$ — Valid signature / Invalid signature

Info-sec is broader than cybersec — Info sec

Cybersecurity — Attacks against cyber devices.

Info security — Protection of info — CIA (of your info)