Protection & Security

Security Violation

Confidentiality → unothorized person can't read data.

Integrity : unothorized " " modaration of data.

availablity : 24/7 available হতে হবে

principle of protection (least privilege)
/
set of permission.

* enough privilege দিলে.
  → permission কমে যাবে
* limit দিলে damage limit হবে.
* process জন্য দিবে and কখন কি দিতে হবে

Domain Structure

Domain is a set of access rights.

Object	Permission
O_3	read write
O_1	read wrote
O_2	execute

Access Matrix

→ View protection as matrix

	object (file / printer)		
		access (1, 2)	
user / D		(D_1)	(O_1)

Program threats → Trojan horse, Logic bomb Virus

System " = worms, Viruses.

Security problem

Threat - Potential security violation.

- attack

Masquerading → অন্যের identify দিয়ে কাজ করা

Session hijacking: Session hack হয়ে যায়, অর্থাৎ session শেষ হবে না

Major Security Levels.

physical → human — OS → Network

Trojan horse: kind of threats, এটা genuine application. app এর মত মনে হবে. virus carrier হবে. but The genuine app system চলবে and destruct করবে. open করে দেবে system entry.

back door → do unauthorized access entry easily.

Worm

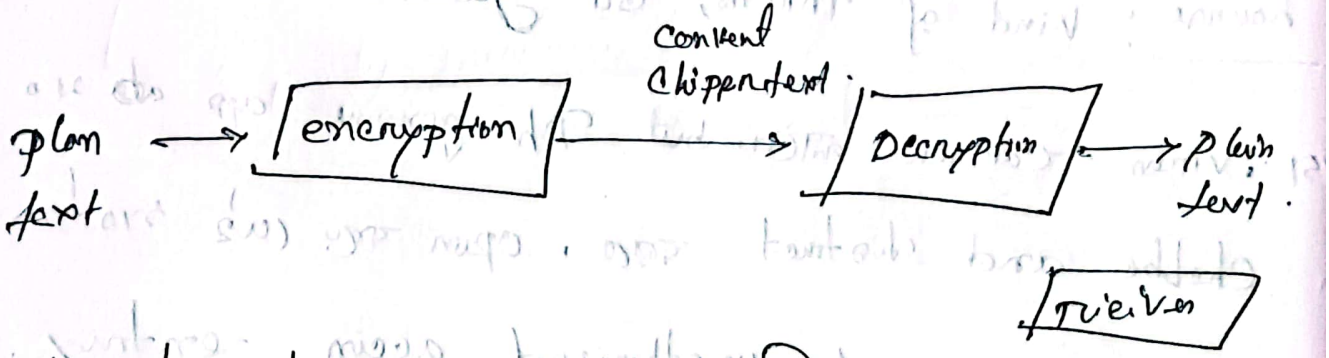
Sub-ch of virus. Its capability to travel without any help from user.

Data transfer করে এবং attach করে travel করে

Cryptography

Plan text → cipher text

(convert করে পাঠানো)



- Symmetric key - same key দিয়ে encry, dcp করে
- asymmetric key - public key
  private key

RSA algo (asymmetric)

In num 2 prime no $p = 13$, $q = 17$, Private key find? (d)
public key 35 (e)

Steps RSA

* calculate $n = p \times q = 13 \times 17 = 221$.
* " $\phi(n) = (p-1) \times (q-1) = 12 \times 16 = 192$
* Chose e value $1 < e < \phi(n) = 1 < e < 192 = 1 < 35 < 192$

So $\gcd(e, \phi(n)) = 1 \Rightarrow \gcd(35, 192) = 1$

* calculate d such $de = 1 \bmod \phi n$.

$= de \bmod \phi(n) = 1$

$= d \cdot 35 \bmod 192 = 1$

value টা এমন হবে d value বসাই যেন 1 আসে দিন

(*) যদি মান দেওয়া না থাকে

$de = 1 \bmod \phi N$

$\therefore de = 1 + k\,\phi(n)$

k = 0 start
0, 1, 2 ....

$\therefore d = \dfrac{1 + k\,\phi(n)}{e} = \dfrac{1 + 0 \times 192}{35} = \dfrac{1}{35}$

Area (1)
আমরা যখন so we 1, 2, 3 use করে direct value (11, 12) এভাবে বসাও
example

RSA algo (asymmetric)

In man 2 prime no $p = 13$, $q = 17$, Private key find? (d)
public key 35 — (e)

Steps RSA

* calculate $n = p \times q = 13 \times 17 = 221$.
* " $\phi(n) = (p-1) \times (q-1) = 12 \times 16 = 192$
* Chose e value $1 < e < \phi(n) = 1 < e < 192 = 1 < 35 < 192$

So $\gcd(e, \phi(n)) = 1 \Rightarrow \gcd(35, 192) = 1$

* calculate d such $de \equiv 1 \bmod \phi n$.

$= de \bmod \phi(n) = 1$

$= d \cdot 35 \bmod 192 = 1$

value বসালে
অর্থাৎ d value হবে
যে 1 আসবে তাই

(*) যদি মান বের না হয়

$de = 1 \bmod \phi N$

$\therefore de = 1 + k\,\phi(n)$

k = 0 start
0, 1, 2 ....

$\therefore d = \dfrac{1 + k\,\phi(n)}{e} = \dfrac{1 + 0 \times 192}{35} = \dfrac{1}{35}$

Ans ① আসা হবে না
So we 1, 2, 3 we
করে direct
value (11, 12) দেখা
example যায়

Defense Depth (Layer)

- Physical controls → Guards, locked doors
- Technical → endpoint security (detection, protection)
  - network Security → VPN, firewall.

administrative controls

It is a strategy that leverage multiple security measures to protect an organization assets