values, where m is the size of the keyword.

$$K=(k_1,k_2,---,k_m,k_1,k_2,---,k_m,----)$$

So, here encryption or decryption is done on one symbol (character or bit) at a time, thus Vigenere Cipher is a Stream Cipher, not a Block Cipher.

(c) Playfair Cipher is Block Cipher because in this cipher, the size of block is $m=2$, i.e, always two characters are encrypted together.

Class After Midsem-2 — 9/10/2023

Euler's Phi function

$$\phi(n)=(p_1^{e_1}-p_1^{e_1-1})+(p_2^{e_2}-p_2^{e_2-1})+---$$

Euler's Theorem

$a^{\phi(n)}=1 \bmod n$

$a, n \Rightarrow$ any integer.

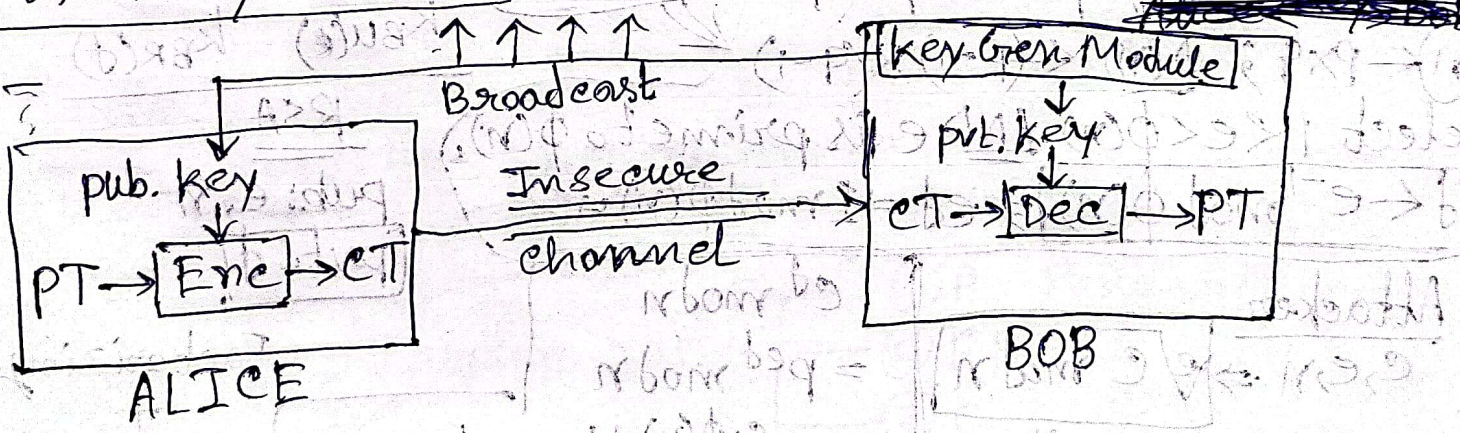
Fermat's little Theorem

$a^{p-1} \bmod p = 1$

$\Rightarrow a^{p-1} \equiv 1 \bmod p$

$a \Rightarrow$ any int, $p \Rightarrow$ prime.

CIA — Asymmetric key Ciphers

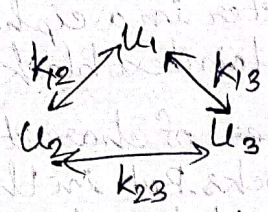


Alice $\xleftrightarrow{\text{key}}$ Bob

P.T.O.

n users

Symmetric



$\#keys = {}^nC_2 = \frac{n(n-1)}{2}$

Not AES questions in endsem

Assymetric

u_1 $k_{1r} \Rightarrow$ private.
$k_{1u} \Rightarrow$ public

$\#keys = n$ pairs.
$= 2n$.

Trapdoor Oneway Function (Similar to knapsack prob.)

$y = f(x)$ Easy $\quad S = w_1x_1 + w_2x_2 - -$

$x = f^{-1}(y)$ Difficult $\quad \begin{matrix} x_1 \\ x_2 \end{matrix} \leftarrow (S, w_1, w_2 - -) \Rightarrow$ NP Prob.

$n \leftarrow p_1 \times p_2 \times p_3$ — Easy
$y \leftarrow f(x)$

$p_1, p_2 - - \leftarrow n$ — Difficult.
$x \leftarrow f^{-1}(y)$

Easy: $y \leftarrow x^k \bmod n$

Difficult: $x \leftarrow y, k, n$?

$x \leftarrow \sqrt[k]{y} \bmod n$

DLP (Discrete logarithm Prob.)

$y \leftarrow x^k \bmod n$
$x \leftarrow y, k, n$?

$a^{\phi(n)} = 1 \bmod n$.

$k' \times k = 1 \bmod \phi(n)$

$\Rightarrow y^{k'} \bmod n = x$

$\Rightarrow y^{k'} = x^{k \times k'} \bmod n$

$\Rightarrow (x^{c \cdot \phi(n)} \cdot x) \bmod n$

$\Rightarrow [x^{\phi(n)} \bmod n]^c \cdot x$

$\Rightarrow x$

$k k' = c \cdot \phi(n) + 1$

RSA

Enc: $C \leftarrow P^e \bmod n$
Dec: $P \leftarrow C^d \bmod n$

RSA key Gen Algo.
Select two large primes p & q.
$n \leftarrow p \times q$; $\phi(n) \leftarrow (p-1) \times (q-1)$
Select $1 < e < \phi(n)$ AND e is prime to $\phi(n)$.
$d \leftarrow e^{-1} \bmod \phi(n) \Rightarrow ed = 1 \bmod \phi(n)$

Key Generation

Alice → Bob
Enc: Dec:
$k_{BU}(e)$ $k_{BR}(d)$

RSA
pub: e, n
pvt: d

Attacker
$C, e, n \Rightarrow \sqrt[e]{C} \bmod n$
Difficult

$C^d \bmod n$
$= P^{ed} \bmod n$
$= P^{c \cdot \phi(n) + 1} \bmod n = P$

Factorizing + Primality Test

Primality

$a^{n-1} \stackrel{?}{=} 1 \bmod n$
If yes →
no →

⇒ Elgamal's

Enc:
$C_1 \leftarrow e_1^r \bmod n$
$C_2 \leftarrow (e_2^r \times$
$[C_1, C_2]$

Key Gen.
Select a
Select e
Select d
$e_2 \leftarrow e_1$

Alice
mess age ← M
Finger Print generator ← Hash
Digest ← D

Eve: M
M to
S.t. M
yet D

Given
③ Co
Given

Hash

Primality Test:

Is n prime?

FERMAT'S TEST

$a^{n-1} \stackrel{?}{=} 1 \bmod n$ (a)

If yes → n is prime.

no → n is composite.

Very few composites which act as primes.

$2^{560} \bmod 561 = 1$ (561)

$\Rightarrow 2^{560} = 1 \bmod 561.$

⇒ Elgamal's Cryptosys:

Enc:

$c_1 \leftarrow e_1^r \bmod p$ (r → secret, p → public)

$c_2 \leftarrow (e_2^r \times P) \bmod p$

$[c_1, c_2]$

Dec:

$c_2 = e_2^r \times P$ $\quad c_1 = e_1^r$

$P \leftarrow [c_2 \times (c_1^d)^{-1}] \bmod n$

$\Rightarrow [e_2^r \times P \times (e_1^{rd})^{-1}] \bmod n$

$\Rightarrow [e_1^{rd} \times P \times e_1^{-rd}] \bmod n$

$\Rightarrow P$ $\quad e_2 = e_1^d$

Key Gen. Algo. El. Gamal:-

Select a Large prime p.

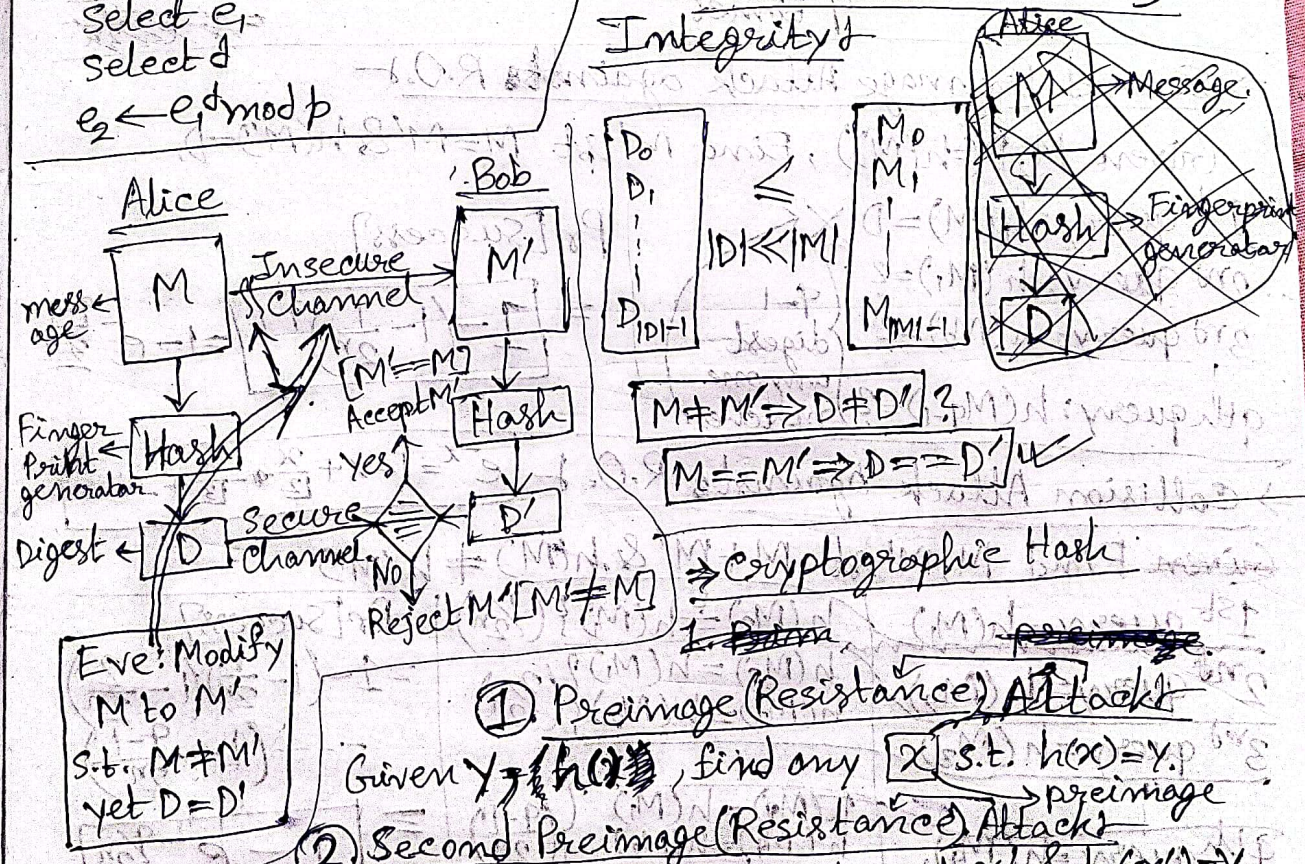
Select e_1

Select d

$e_2 \leftarrow e_1^d \bmod p$

Class After Midsem-3

Integrity:



⇒ Cryptographic Hash

1. ~~Preimage~~ ~~preimage~~.

① Preimage (Resistance) Attack:

Given $y = h(x)$, find any x s.t. $h(x) = y$.

② Second Preimage (Resistance) Attack:

Given y, x, h() st. $y = h(x)$, find x' s.t. $x \neq x'$ & $h(x') = y$.

③ Collision (Resistance) Attack:

Given h(), find x, x' s.t. $h(x) == h(x')$.

~~Has~~ Cryptographic Hash:

① P. Resistance

② S.P. "

③ C. "

⇒ Random Oracle (R.O.)

Message	Digest (n-bits)
M_1	D_1
M_2	D_2

$M_2 = M_1$? yes → D_1, No →

Digest = n-bits.

#digests = 2^n

Allowed: (q) queries

⇒ Preimage Attack against R.O.

Given D, find M s.t. $h(M)=D$

Pr[Find an M within q queries]

$Pr[h(M_1)=D] = \frac{1}{2^n}$,

$Pr[h(M_2)=D] = \frac{1}{2^n}$,

$Pr[h(M_q)=D] = \frac{1}{2^n}$

$\Rightarrow Pr[h(M_1)=D \vee h(M_2)=D \vee \dots h(M_q)=D]$

$\Rightarrow 1 - Pr[h(M_1)\neq D \wedge h(M_2)\neq D \wedge \dots h(M_q)\neq D]$

$\Rightarrow 1 - \underbrace{\left(1-\frac{1}{2^n}\right) * \left(1-\frac{1}{2^n}\right) * \dots \left(1-\frac{1}{2^n}\right)}_{q \text{ times}} \Rightarrow \boxed{1-\left(1-\frac{1}{2^n}\right)^q} \approx \frac{q}{2^n}$

⇒ Second Preimage Attack against R.O.

Given M, $D(=h(M))$, Find M' s.t. $M=M'$ & $h(M')=D$.

1st query: $h(M)=D$ ✗

2nd query: $h(M_1)=?$

3rd query: $h(M_2)=?$

$(q-1)$ digest any one matches.

qth query: $h(M_{q-1})=?$

$Pr[\text{Success}] = \boxed{1-\left(1-\frac{1}{2^n}\right)^{q-1}} = 1-e^{-\frac{q-1}{2^n}}$

⇒ Collision Attack against R.O.

$e^{-x} = 1 - x + \frac{x}{|2} - \frac{x}{|3} + \dots$

Find M, M' s.t. $M \neq M'$ & $h(M) = h(M')$

1st query $= h(M_1)$

2nd query $= h(M_2)$ — $h(M_2) \stackrel{?}{=} h(M_1)$ $\left(\frac{1}{2^n}\right)$

3rd query $= h(M_3)$ — $h(M_3)=h(M_1)$, $h(M_3)=h(M_2)$ $\left(\frac{2}{2^n}\right)$

qth query $= h(M_q)$ — $h(M_q)=h(M_1)$, $h(M_q)=h(M_2)$, $h(M_q)=h(M_{q-1})$ $\left(\frac{q-1}{2^n}\right)$

$Pr[\text{Success}] = 1-\left(1-\frac{1}{2^n}\right)\left(1-\frac{2}{2^n}\right)\dots\left(1-\frac{q-1}{2^n}\right) \equiv \boxed{1-e^{-\frac{q}{2^n}}}$

If for q queries, $q\,Pr[\text{Success}] = 0.5$

For Collision Attack

$1-e^{-\frac{q}{2^n}} = 0.5$

$\Rightarrow e^{-q/2^n} = 0.5$

$\Rightarrow +q/2^n = \ln(0.5) = -0.69$

$\Rightarrow q = 0.69 \times 2^n$

For S.P.A.

$1-e^{-\frac{q-1}{2^n}} = 0.5$

$\Rightarrow q = 0.69 \times 2^n + 1$

For P.A.

$q = (0.69)\frac{1}{2} \times 2^{n/2}$

If collision resistant then all 2 attacks resistant too.