Ron Rivest
Adi Shamin
Leonand Adleman

RSA Cnyptosystem: a widely used public key cnyptognaphic system that facilitate s secune data tnansmission.

key components:

1) public key : {n, e}
2) pnivate key : {d, n}

Math Step:

1) Given, p. q (lange pnime numbens)
2) $n = p \times q$
3) $\phi(n) = (p-1)(q-1)$
4) choose e such that
   a) $1 < e < \phi(n)$
   b) $\gcd(e, \phi(n)) = 1$
5) find d, $d \times e \equiv 1 \pmod{\phi(n)}$
6) Encnyption, $C = M^e \bmod (n)$ → use public key
7) Decnyption, $m = C^d \bmod n$. → use pnivate key

Example: Let, $p = 61$, $q = 53$

$n = 61 \times 53 = 3233$

$$\phi(n) = (61-1)(53-1) = 3120$$

Suppose, $e = 17$

$\because \gcd(17, 3120) = 1$

$$d = 17^{-1} \bmod 3233$$

$$= 2092$$

Let $m = 65$. $\quad C = 65^{17} \bmod 3233$ —— ①

$$M = (65^{17})^{2092} \bmod 3233 \quad \text{—— ②}$$

$17 = 8 + 4 + 2 + 2 + 1$

① → $\therefore \quad 65^{17} = (65^8 \cdot 65^4 \cdot 65^2 \cdot 65^2 \cdot 65^1) \bmod 3233$

$$= (1547 \times 1232 \times 992^2 \times 65) \bmod 3233$$

$65^1 \bmod 3233 = 65$

$65^2 \bmod n = 2790$

$= 4225 \bmod n$

$= 992$

$65^4 \bmod n$

$= (992 \times 992) \bmod n$

$= 1232$

$65^8 \bmod n$

$= (2237)^2 \bmod n$

$= 1547$

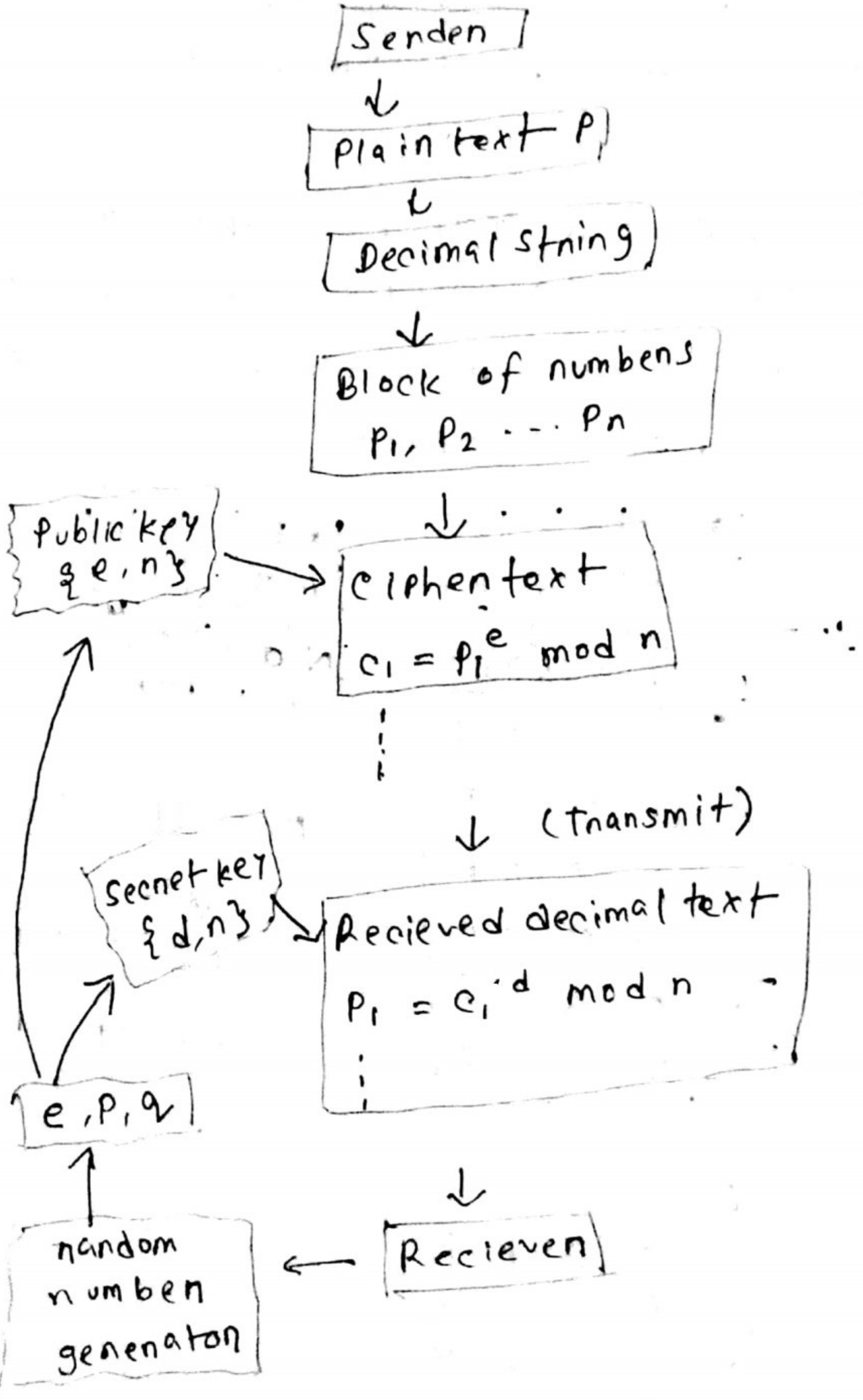
$\therefore C = 2790$

$M' = 2790^{2092} \bmod 3233$

$= 2699$

$\therefore M \neq M'$

* General pipeline :



* Play fain ciphen :

- symmetnic encyption
- dignam substitution ciphen

↓

2

ques TT * suppose a gnoup of people agneed upon a key, k = "puzzLE". now find the ciphentext of the plaintext, m = "LITTLE" using playfain ciphen.

→

P	U	Z	L	E
A	B	C	D	F
G	H	I/J	K	M
N	O	Q	R	S
T	V	W	X	Y

k =

m = LI TT LE

= LI TX TL EX

ZK VY XP LY

* Diffie - Hellman key exchange protocol:

→ 2 person share a value on public channel {p, g}

p → large prime
g → base

→ each person chooses secret number (a/b) and

→ compute public keys value:
$g^a \bmod p$; $g^b \bmod p$

→ exchange public value

→ computed shared secret:
$(g^a)^b \bmod p == (g^b)^a \bmod p$.

Pros of IPsec (Internet Protocol security)
→ Internet secure at IP layer

(1) provides strong encryption and authentication to protect data
(2) ensures data is not altered.
(3) works well with existing net/app and protocols without modification
(4) flexible and Transparent

* Playfain: K = ASGHARD

M = GROOT

GR OX OT

RD QV PU

K =					
	A	S	G	R	D
	B	C	F	F	H
	I/J	K	L	M	N
	O	P	Q	T	U
	V	W	X	Y	Z

* Elgamal Cryptosystem:

Given, $p = 7$, $g = 3$

(a) (1) select private key. $1 \leq sk \leq p-2$

$1 \leq sk \leq 7-2$

$\therefore \boxed{sk = 5}$

(2) $P_k = g^{sk} \bmod p$

$y = 3^5 \bmod 7$

$= 243 \bmod 7 = 5$

Ans: $\therefore$ public key $(p, g, y) = (7, 3, 5)$

$\therefore$ private key, $x = 5$

(b) $P_k : (p = 7, g = 3, y = 5)$, $m = 13$

random k : $1 \le k \le p-2$ $\therefore k = 4$

$c_1 = g^k \bmod p = 3^4 \bmod 7 = 4$

$c_2 = m \cdot y^k \bmod p = 13 \cdot 5^4 \bmod 7 = 5$

$\therefore (c_1, c_2) = (4, 5)$

* Why are RAIDs used?

→ Redundant Annay of Independent Disks.

→ data is stoned in multiple disks. If 1 disk fails, no data loss.

→ data neliabbility and availability thnough redundancy and fault tolenance

→ distnibute data across multiple disks