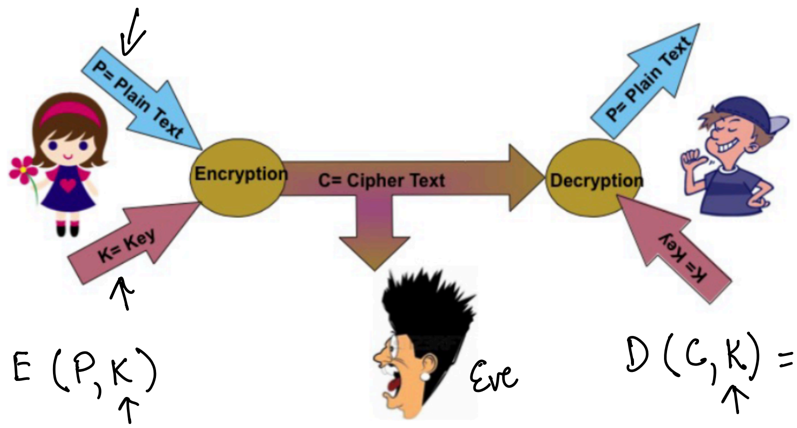
This Lecture:

-Classical Cryptography

- Symmetric Cryptography
- Assymetric Cryptography
    - RSA Encryption Limitation
- Vernam Cipher (One Time Pad)
- Quantum One Time Pad

[Classical Cryptography]

[Symmetric Cryptography]

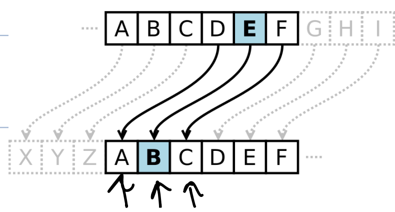


$C = E(P, K)$

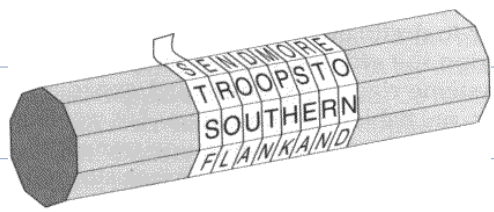
Eve

$D(C, K) = P.$

Caeser Cipher 100 BC

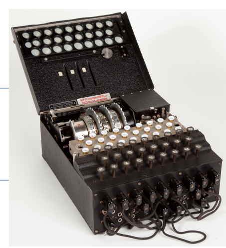


Scytale   7 BC



The Enigma Machines 20 AD

1923

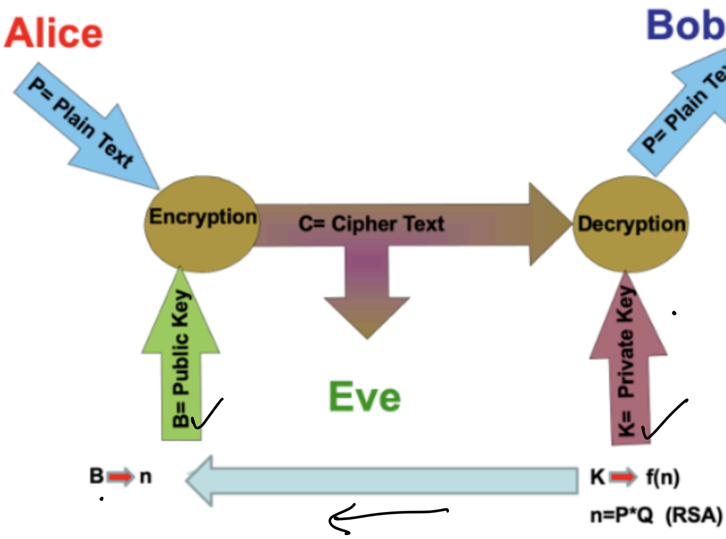


1932 - 33.

1940.

[Asymmetric Cryptography]()

$B \& K.$



generates

$B \to n.$

$K \to f(n).$

Knowing n computationally difficult to get f(n).

One way Functions used:

- Integer factorization problem $n = p \times q.$
- The discrete logarithm problem
- Elliptic-curve discrete logarithm problem

RSA Encryption: Rivest-Shamir-Adleman 1977

$n = p \times q$. $\quad \mathcal{E}: n \quad D: p, q$.

- select two prime numbers
- calculate $n = p \times q$.
- Public Key (e, n). $\quad C = M^e \bmod n$.
- Private Key (d, n). $\quad M' = C^d \bmod n$. ✓

$M' = M$.

- Generate e.

$\varphi(n) = (p-1)(q-1)$

  - $1 < e < \varphi(n)$.
  - e should not be a factor of n.

- Generate private Key (d, n).

For given $n, p, q,$ & e, there is a unique d.

s.t. d is inverse of $e \pmod{\varphi(n)}$.

$ed = 1 \bmod \varphi(n)$

$ed - 1 = K\varphi(n)$. $\quad \Rightarrow ed = 1 + K\varphi(n)$

Then $M' = C^d \mod n.$

$$= M^{ed} \mod n.$$

$$= M^{1+K\varphi(n)} \mod n.$$

$$= M \cdot \underbrace{M^{K\varphi(n)}}_{1} \mod n.$$

$$M' = M.$$

Example:

let $p = 53 \quad q = 59.$

$\therefore n = \underline{p \times q} = 53 \times 59 = 3127.$

$\varphi(n) = (p-1)(q-1) = 52 \times 58 = 3016.$

$\therefore$ Select $e = 3.$

$\therefore$ Public Key is $(n, e) = (3127, 3).$

$\therefore$ Private Key:

$ed - 1 = K\varphi(n)$ ✓

$d = (K\varphi(n) + 1)/e.$

$K=2 \quad d = (2 \times 3016 + 1)/3 = 2011.$

Private Key is $(n, d) = (3127, 2011).$

Send the Message: Hi.

- Convert Message into a number.

a	b	c	d	e	f	g	h	i	
1	2	3	4	5	6	7	8	9.	Everyone knows.

Hi $\rightarrow$ 89 = M.

- Encrypted message.

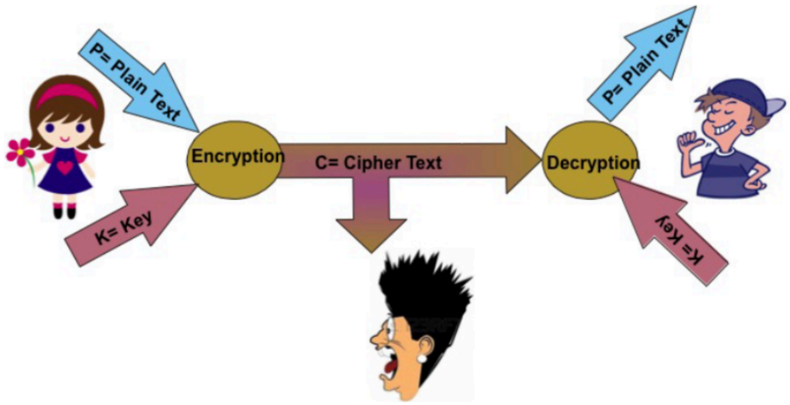
$$C = M^e \bmod n.$$
$$= 89^3 \bmod 3127$$
$$= 704969 \bmod 3127$$
$$= 1394$$

Decrypt: $M' = C^d \bmod n.$
$$= (1394)^{2011} \bmod (3127)$$
$$= 89$$
$$= M.$$

Difficult to break if difficult to find prime factors of n.

Shor's algorithm (quantum algo) can break the code!

Symmetric Cryptography



One Time Pad: The Vernam Cipher 1926 (Perfect Secracy)

P = 0 1 1 0 1 0 0 1 0 1 ✓

K = 1 0 1 1 1 0 1 1 0 0

C = P $\oplus$ K

1 1 0 1 0 0 1 0 0 1

$D = C \oplus K = P \oplus K \oplus K = P.$

A 000

B 001

C 101

ABC

000 001 101.

- Perfectly secure iff.
  - K is random.
  - K is secret
  - As long as the message.
  - Used only once.

QKD solves the problem of Key distributed.

Quantum One Time Pad:

$0, 1 \longrightarrow |0\rangle, |1\rangle.$

standard basis $\{|0\rangle, |1\rangle\}$. in Z- basis

$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ ✓

$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. ✓

Hadmard basis set $\{|+\rangle, |-\rangle\}$.

$\langle 0, 1\rangle = \langle + | - \rangle = 0.$

$\{0, 1\}.$

$X|0\rangle = |1\rangle \qquad X|M\rangle = |M \oplus 1\rangle.$

$X|1\rangle = |0\rangle$

$|E\rangle = X_{\underline{K}}|M\rangle \qquad K = 1.$

$\{|0\rangle, |1\rangle\} \qquad \{|+\rangle, |-\rangle\}.$

<u>Z - operator</u>:

$Z|0\rangle = |0\rangle \qquad Z|+\rangle = |-\rangle$

$Z|1\rangle = -|1\rangle \qquad Z|-\rangle = |+\rangle$

$K_1 \; \{0, 1\}$.
$K_2 \; \{0, 1\}$.

Encryption:

$$|E\rangle = Z_{K_2} X_{K_1} |M\rangle$$

Decryption: $$|D\rangle = X_{K_1} Z_{K_2} |E\rangle$$
$$= X_{K_1} \underbrace{Z_{K_2} Z_{K_2}}_{1} X_{K_1} |M\rangle$$
$$= X_{K_1} X_{K_1} |M\rangle$$
$$= |M\rangle.$$

Sender & Reciever should have same K_1 & K_2.

Quantum one-time pad gives no advantage over classical one-time pad.

So we got QKD.