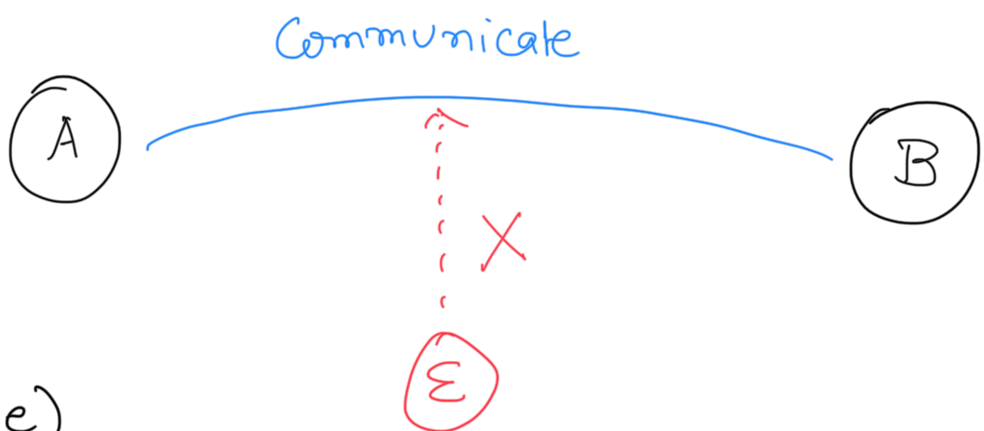
LECTURE 1 (Dec 27, 2023)

RAKVI

Textbook: Guide to Elliptic Curve Cryptography

Authors: Darrel Hankerson
Alfred Menezes
Scott Vanstone

CRYPTOGRAPHY



(Message)

I AM AT ROSE PARK

(Basic Cipher) +3

L DP DW URVH SDUN

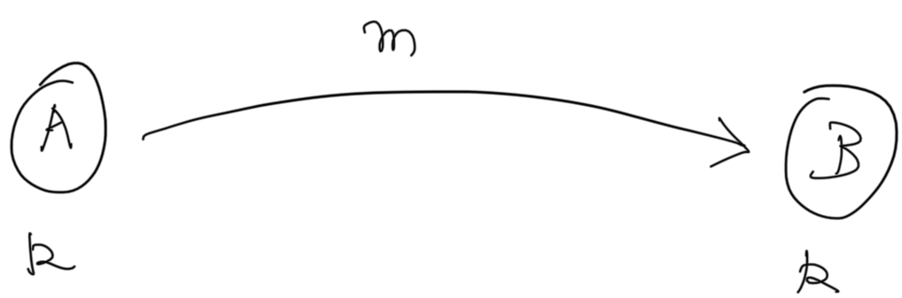
↓ Encrypted message (ciphertext)

B's job is to decrypt this message

Key Go back 3 letters !

Problem is this is easy to break

This cipher was an example of symmetric key cryptography.



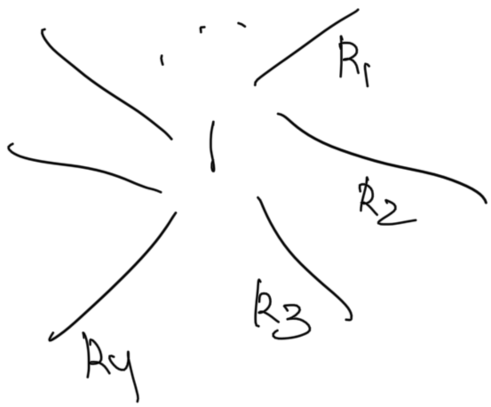
A will use an encryption algorithm to create $C = Enc(m, k)$

B will receive C and then recover

$$m = Decryption(C, k)$$

Managing keys can require lot of computing memory.

Group of N people



An alternative is to use <u>Public-key cryptography</u>.

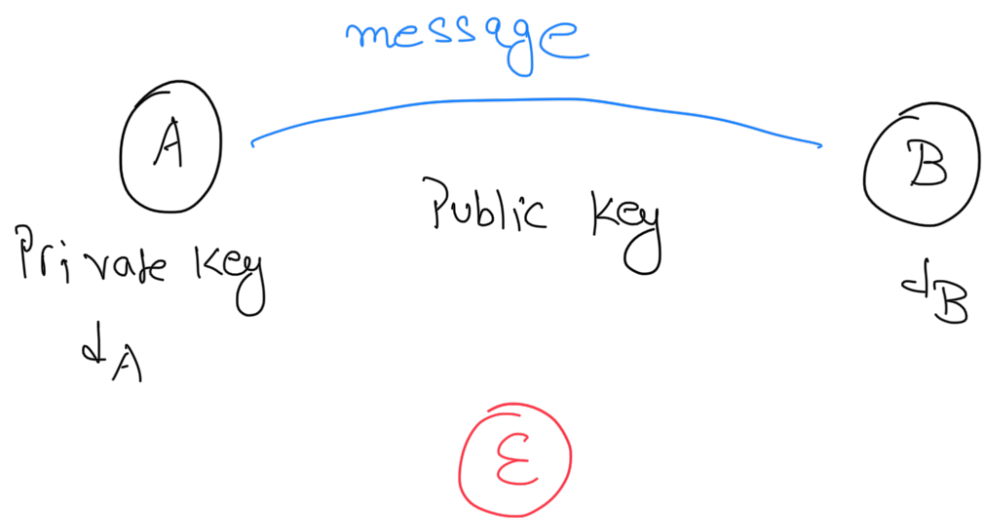
(1) RSA protocol

Rivest

Shamir

Adleman (proposed in 1977)

Check this?



Underlying mathematical problem is <u>hard</u> to solve.

1. l : Security parameter (bit length)

Generate a public key, P_R and a private key d_A

2. Randomly select two primes p, q

3. Compute $pq = n$ and $\phi = (p-1)(q-1)$

ϕ → Euler's Totient function

<u>Aside:</u> $\phi(n)$ is the number of integers between 1 and n which are coprime to n.

$n = 3 \qquad \phi(3) = 2$

1 2 3

$n = 6$

1 2 3 4 5 6

$\phi(6) = 2$

$n = pq$

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

---

(4) Select an arbitrary number $1 < e < \phi$ s.t $\gcd(e, \phi) = 1$

(5) Compute d s.t $\boxed{de \equiv 1 \pmod{\phi}}$

Aside:

$7 \equiv 1 \pmod{3}$

$5 \equiv 2 \pmod{3}$

6 Public key (n, e)

Private key d

$$n \overset{\text{Hard}}{=} pq$$

Relies on diffi culty of integer factorisation

How does RSA encryption work?

Start with message $0 \le m \le n-1$

I already know public key (n, e)

Ciphertext $C = m^e \pmod{n}$

Decryption Private key d

All B has to do is $C^d \pmod{n}$

$$= (m^e)^d \pmod{n}$$

$$= m^{ed} \pmod{n}$$

$L = m \pmod{n}$

This uses group structure information.

(We will see this in coming lectures!)

Discrete logarithm systems

Elliptic Curve Cryptography (ECC)

Elliptic Curve

Example $\quad y^2 = x^3 + 1$

Find all its roots, they should be distinct

$y^2 = (x-1)^3 \quad \times$ (not an EC!)

In general $\quad y^2 = x^3 + ax + b$

$$\boxed{4a^3 + 27b^2 \neq 0}$$

We will focus on Elliptic Curves over finite fields in this course.

$$y^2 z = x^3 + 2xz^2 + 4z^3 \text{ (Projective)}$$

Example: (Affine) $y^2 = x^3 + 2x + 4$ over $\mathbb{F}_7$

$$\boxed{4a^3 + 27b^2 \neq 0}$$

finite field that has 7 members

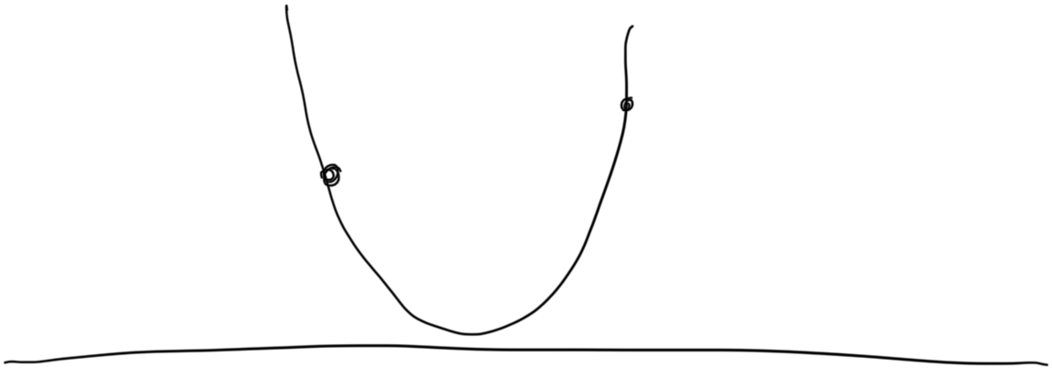
$$\{0, 1, 2, 3, 4, 5, 6\}$$

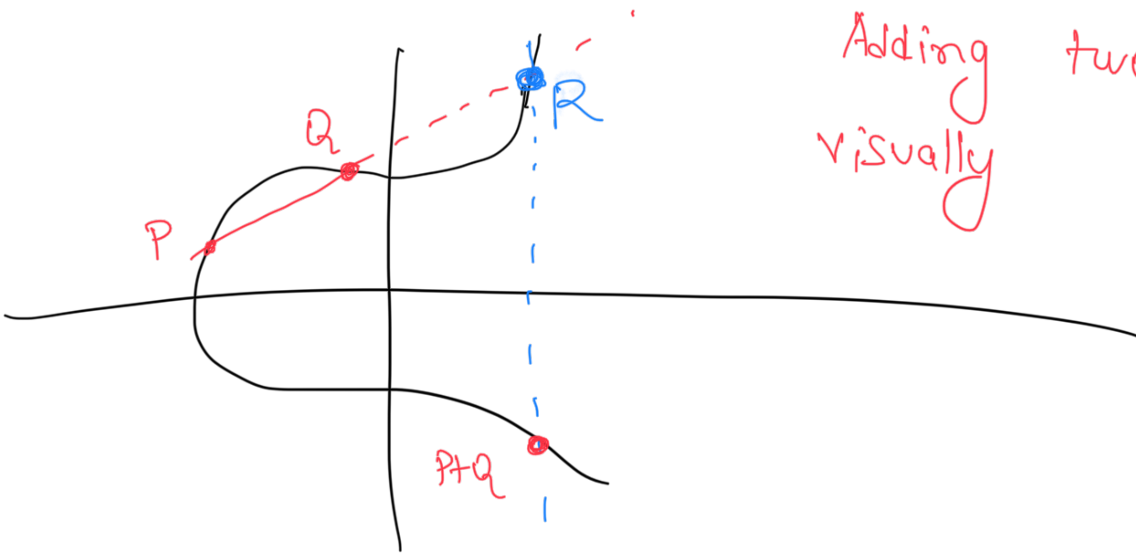
$$1 + 6 = 7 \pmod 7$$
$$= 0$$

$$1 \cdot 6 = 6 \pmod 7$$

$$\{\infty, (0,2), (0,5), (1,0), (2,3), (2,4) \text{ - - - - } \}$$

One can <u>add</u> two points on elliptic curves.





Adding two points visually

$\mathcal{E}$ over a finite field $\mathbb{F}_p$ (denotes finite field that consists of p elements)

P point on $\mathcal{E}$ $\quad \underbrace{P+P+\cdots+P}_{n} = \underset{\text{identity}}{\mathcal{O}}$

$$\langle P \rangle = \{\infty, P, 2P, 3P, \ldots, (n-1)P\}$$

↓

group generated by P

(p, E, P, n) Parameters

Want to generate

Public key Q

Private key d

1. Select a number $1 \le d \le n-1$
2. Compute $Q = dP$

Recovering d from Q & P is hard!

Encryption (p, E, P, n) Q, message m

1. Represent m as a point on E
2. Select a $1 \le k \le n-1$
3. Compute kP

4 Compute $m + RQ$

Return $(RP, m + RQ)$ as my cipher text.

Decryption d private key

Compute $m + RQ - dRP$

$m + RQ - RQ$

Recovered m