CRYPTOGRAPHY:

ASYMMETRIC ENCRYPTION

→ our goal now is how to establish a shared secret key

ONLINE TRUSTED THIRD PARTY (TTP)

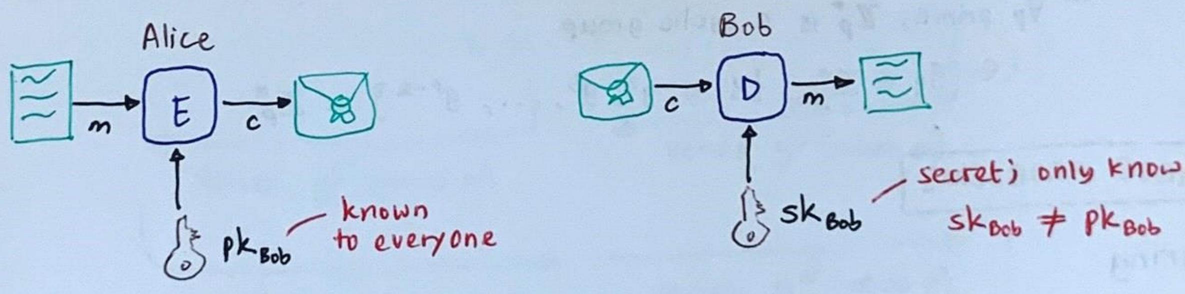
- Users $U_1, U_2, U_3, \dots, U_n, \dots$

  Each user U_i has a shared secret key K_i w/ the TTP
- U_i and U_j can establish a key $K_{i,j}$ w/ the help of the TTP
- $\{m\}_K$ denotes the symmetric encryption of m under the key K

↓ establish a shared secret key w/o a TTP

PUBLIC-KEY CRYPTOGRAPHY

- Key generation algo. $G \rightarrow K \times K$ – generates 2 keys: PRIVATE KEY, PUBLIC KEY
- Encryption algo. $E \rightarrow K \times M \rightarrow C$ – uses public key
- Decryption algo. $D \rightarrow K \times C \rightarrow M$ – uses private key



NUMBER THEORY

- Every $n \in \mathbb{N}$ has a unique factorization as a pdt. of prime numbers
- a and b in $\mathbb{Z}$ are relative primes if they have no common factors
- Euler fn $\phi(n)$ is the no. of elems. that are relative primes w/ n

$$\phi(n) = |\{m \mid 0 < m < n \text{ and } \gcd(m, n) = 1\}|$$

↳ For p prime: $\phi(p) = p - 1$

For p and q primes: $\phi(p \cdot q) = (p-1)(q-1)$

- Let $n \in \mathbb{N}$. We define $\boxed{\mathbb{Z}_n = \{0, \dots, n-1\}}$

$\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}_n, \boxed{a \equiv b \pmod{n}} \Leftrightarrow \exists k \in \mathbb{N}.\ a = b + k \cdot n$

MODULAR INVERSION

- The inverse of $x \in \mathbb{Z}_n$ is $y \in \mathbb{Z}_n$ s.t. $\boxed{x \cdot y \equiv 1 \pmod{n}}$

e.g. 7^{-1} in $\mathbb{Z}_{12} = 7 \rightarrow 7 \times 7 - 4 \times 12 = 1$

Inverse of 7 mod 12

4^{-1} in $\mathbb{Z}_{12}$ = 4 has no inverse in $\mathbb{Z}_{12}$

> Let $n \in \mathbb{N}$, $x \in \mathbb{Z}_n$. x has an inverse in $\mathbb{Z}_n$ iff $\gcd(x, n) = 1$
> relative primes

- Let $n \in \mathbb{N}$, we define $\boxed{\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n \mid \gcd(x, n) = 1\}}$ → all the numbers that have inverses

e.g. $\mathbb{Z}_{12} = \{1, 5, 7, 11\}$

Note thr. $|\mathbb{Z}_n^*| = \phi(n)$

- EULER THM. $\forall n \in \mathbb{N}, \forall x \in \mathbb{Z}_n^*$, if $\gcd(x, n) = 1$ then $x^{\phi(n)} \equiv 1 \pmod{n}$

↳ $\forall p$ prime, $\mathbb{Z}_p^*$ is a cyclic group

i.e. $\exists g \in \mathbb{Z}_g^*, \{1, g, g^2, g^3, \dots, g^{p-2}\} = \mathbb{Z}_p^*$

INTRACTABLE PROBLEMS

1) Factoring

2) RSA Problem
   - input — n s.t. $n = p \cdot q$ w/ $2 \leq p, q$ primes
     - e s.t. $\gcd(e, \phi(n)) = 1$
     - $m^e \bmod n$
   - output — m

3) Discrete Log
   - input — prime p, generator g of $\mathbb{Z}_p^*$, $y \in \mathbb{Z}_p^*$
   - output — x s.t. $y = g^x \pmod{p}$

4) DHP
   - input — p prime
     - g generator of $\mathbb{Z}_p^*$
     - $g^a \pmod{p}$
     - $g^b \pmod{q}$
   - output — $g^{ab} \pmod{p}$

DIFFIE-HELLMAN (DH) PROTOCOL

- Assumption: The DHP is hard in $\mathbb{Z}_p^*$

The security of DH protocol is based on ascmn tht. it is difficult for attacker to determine key K from the public parameters and the eavesdropped values X and Y

- Start by fixing a large prime p and g generator of $\mathbb{Z}_p^*$

Alice

$a \xleftarrow{r} \{1, \ldots, p-1\}$ random no.

Bob

$b \xleftarrow{r} \{1, \ldots, p-1\}$ random no.

Bob → Alice: sends $g^b \pmod p$

Alice → Bob: replies w/ $g^a \pmod p$

Alice:

$k_{AB} = (g^b)^a \pmod p$

$= g^{ab} \pmod p$

Bob:

$k_{AB} = (g^a)^b \pmod p$

$= g^{ab} \pmod p$

- is vulnerable to a man-in-the-middle attack

Alice

$a \xleftarrow{r} \{1, \ldots, p-1\}$

Attacker

$a' \xleftarrow{r} \{1, \ldots, p-1\}$

$b' \xleftarrow{r} \{1, \ldots, p-1\}$

Bob

$b \xleftarrow{r} \{1, \ldots, p-1\}$

Attacker → Alice: sends $g^{b'} \pmod p$

Bob → Attacker: sends $g^b \pmod p$

Alice → Attacker: replies w/ $g^a \pmod p$

Attacker → Bob: sends $g^{a'} \pmod p$

$k_{AB} = g^{ab'} \pmod p$

$k_B = g^{ba'}$

$k_A = g^{a'b}$

$k_{BA} = g^{a'b} \pmod p$

DH Protocol Steps:

1) Bob picks a random (+)ve no. b in $\mathbb{Z}_p$ and uses it to compute $X = g^b \bmod p$. He sends X to Alice.
2) Alice picks a random (+)ve no. a in $\mathbb{Z}_p$ and uses it to compute $Y = g^a \bmod p$. She sends Y to Bob.
3) Bob computes the secret key as $K_1 = Y^b \bmod p = g^{ab} \pmod p$
4) Alice computes the secret key as $K_2 = X^a \bmod p = g^{ab} \pmod p$

Public params: p, g, X, Y

RSA CRYPTOSYSTEM

→ allows a potential message receiver, Bob, to create his public & priv. keys

1) Bob generates 2 large, random prime no. p and q → $n = pq$

2) Bob picks a number e that is relatively prime to $\phi(n)$

3) Bob computes $d = e^{-1} \bmod \phi(n)$

4) Bob's $\boxed{\text{public key}}$ is the pair (e, n) and his $\boxed{\text{priv. key}}$ is d

5) Given Bob's public key, Alice can encrypt a message M for him:

$$\boxed{C = M^e \bmod n}$$

6) To decrypt, Bob performs a modular exponentiation

$$\boxed{M = C^d \bmod n}$$

SECURITY

→ is closely tied to factoring n, which would reveal values of p and q

→ Since this is an intractable problem, we can rely on the security of RSA provided we use a large enough modulus.

ELGAMAL (EG) CRYPTOSYSTEM

1) Bob chooses a random large prime no. p and finds a generator g for $\mathbb{Z}_p$

A number g in $\mathbb{Z}_p$ is a generator if for each positive int. i in $\mathbb{Z}_p$, there is an int. k such that $i = g^k \bmod p$.

2) Bob picks a random num. x between $1 \dots p-2$ and computes $\boxed{y = g^x \bmod p}$

3) Bob's $\boxed{\text{public key}}$ is the triple (p, g, y) and his $\boxed{\text{priv. key}}$ is x

4) Given Bob's public key, she generates random num. k between $1 \dots p-2$ and uses modular multiplication & exponentiation to compute 2 nums:

$$a = g^k \bmod p$$
$$b = My^k \bmod p$$

The encryption of M is the pair (a, b)

5) To decrypt, Bob computes:

$$M = b(a^x)^{-1} \bmod p$$