Assymetric Cryptography

Limitation of Symmetric Crypt.

- Sender & receiver should meet in person!
- Need a key $\forall$ pair of agents who want to communicate securely.
- How to share a secret key securely between two agents over insicure net.

Abelian Groups

- It is a pair $(G, \circ)$ where:
  - G is a set
  - $\circ$ is a binary operation such that:
    - * Closure: $\forall g, h \in G$, $g \circ h$ is in G
    - * E an identity $e \in G$ such that $e \circ g = g$ for $g \in G$
    - * Every $g \in G$ has an inverse $h \in G \mid h \circ g = e$
    - * Associativity: $\forall f, g, h \in G$, $f \circ (g \circ h) = (f \circ g) \circ h$
    - * Commutativity: $\forall g, h \in G$, $g \circ h = h \circ g$
- The order of G is # of elements in G.

Group Operation

- Can be written multiplicatively:
  - * $g \circ h = gh$
  - * Does not mean it is integer addition or mul.
- Identity is either 1 or 0
- Inverse of group elem g is g^{-1}
- Group exponentiation: g^m, apply operation m times to g

Cyclic Groups

- Let $(G, \cdot)$ be a finite group of order q
- Let g be some element of G.
- Consider set $\langle g \rangle = \{g^0, g^1, \ldots\}$.
- We know $g^q = 1 = g^0$ meaning set has $\leq q$ elems.
- If set $\langle g \rangle$ has q elems, then g is a generator of $(G, \cdot)$
- A generator g "generates" all elements in the group when group op is applied to itself multiple times.
- If Group has a generator then we say this is a cyclic group.

Diffie-Hellman Key Exchange

$\rightarrow (\mathbb{Z}_p^*, *)$ with generator g where p is prime.

Alice

1. Choose a random $x \in \mathbb{Z}_p^*$
2. Compute $g^x \bmod p$
3. Compute $(g^y)^x \bmod p$

$g^x \bmod p$ →

← $g^y \bmod p$

Bob

1. Choose a random $y \in \mathbb{Z}_p^*$
2. Compute $g^y \bmod p$
3. Compute $(g^x)^y \bmod p$

- The key exchange is secure under Computational Diffie-Hellman assumption
- Given g^x it is **hard** to find x (DL problem)
- Given g^x & g^y it is **hard** to find g^{xy} (Computational DH)
- Given g^x, g^y, g^{xy} & a random 2, it is **hard** to distinguish g^{xy} from 2. (Decisional DH)

Note!

DH key exchange makes it infeasible for an eavesdropper to learn key exchanged!

Asymmetric Encryption

- Every secret key **sk** has an **inverse public key**
- It is **hard** to compute sk from public information (including pk)
- The **public key** can be used to **create a ciphertext** by encrypting a plaintext. The **secret key** can be used to **decrypt the ciphertext** back to plaintext.
- Goals:
  - Guarantee message confidentiality
  - Provide provable security under well studied mathematical assumptions.

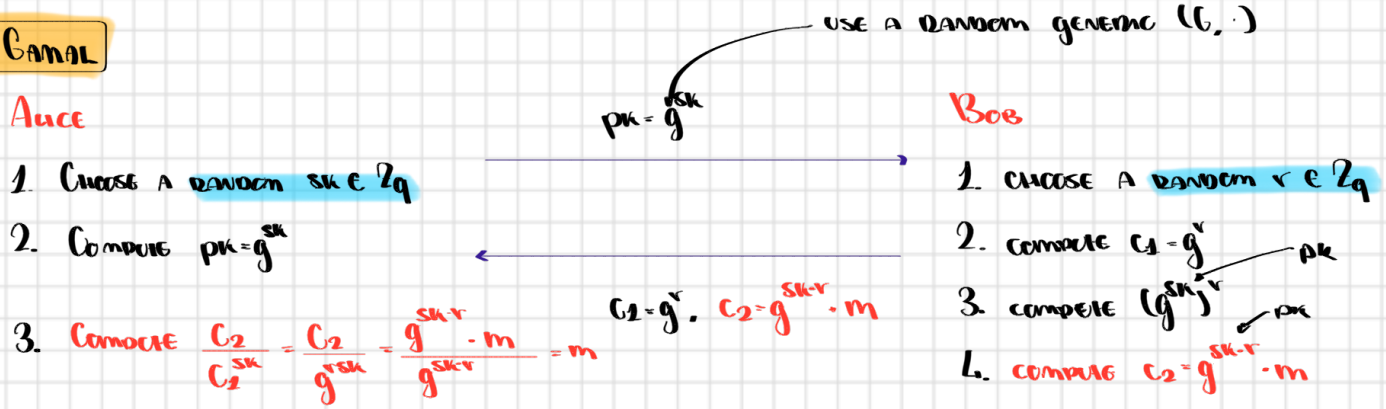
  Confidentiality is guaranteed as long as mathematical problem is "hard"

- Key Gen = (sk, pk) a pair
- Encryption $E(m, pk)$. Allows ciphertext c given m & pk
- Correctness $D(E(m, pk), sk) = m$
- Security: if sk' is not corresponding to pk, then correctness is useless for m.
- ElGamal, RSA...
- Length 256 - 4096
- Slower than symmetric crypto

Note!

Given a key pair (sk, pk) and a ciphertext $E(m, pk) = c$, an adversary who does not know sk learns no info about m.

El Gamal



5 steps:

0. Generate a random sk ∈ Z_q
2. Compute $pk = g^{sk}$
3. Encrypt
   1. Choose a random r ∈ Z_q
   2. Compute $c_1 = g^r$
   3. Compute $c_2 = m \cdot pk^r = m \cdot (g^{sk})^r$
   4. Output $C = (c_1, c_2)$

Decription

Compute:

$$\frac{c_2}{c_1^{sk}} = \frac{c_2}{g^{r \cdot sk}} = \frac{g^{sk \cdot r} \cdot m}{g^{sk \cdot r}} = \boxed{m}$$

Digital Signature

- Goal: integrity + authenticity
- Based on asymmetric crypto
  - Secret/signing key to create the signature
  - Public/verification key to verify the signature
- An algo $\sigma = sign(m, sk)$
- An algo $d = ver(\sigma, m, vk)$
- $(sk, vk) = keygen()$
- Correctness: $ver(sign(m, sk), m, vk) = true$

El Gamal Signatures

- Gen random sk & compute $pk = g^{sk} \bmod p$
- Sign:
  - Choose a random $k \in Z_p$ such that k is relatively prime to p-1
  - Compute $r = g^k \bmod p$
  - Compute $s = (H(m) - sk \cdot r) k^{-1} \bmod (p-1)$, if s=0 go to step 1
  - Output (r, s)
- Verify:
  - Check that $0 < r < p$ & $0 < s < p-1$

- Check that $g^{H(m)} = pk^r r^s$
- Output 1 iff all checks pass, output 0 otherwise.