Asymmetric Cryptography

Lecture 4

RSA cryptosystem

- Let p, q be two different primes and $n = pq$ and $\varphi = \varphi(n) = (p-1)(q-1)$;
- Let e, d be to integers such that $ed \bmod \varphi = 1$.
- $\forall m \in \{0, 1, \ldots, n-1\}$, if $c = m^e \bmod n$ then $m = c^d \bmod n$, and vice versa.

Discrete Logarithm Problem – DLP

- $F_p, p \in \wp$ is a field with a prime number of elements, finite field.

Proposition. Let $p \in \wp, \exists g \in F_p, n \in \mathbb{N}$: $\forall x \in F_p, x \equiv g^n \ (mod\ p)$. g is called a primitive element or a generator.

Definition (DLP). Let g be a primitive root for F_p and let h be a nonzero element of F_p. The DLP is the problem of finding an exponent x such that $g^x \equiv h$ (mod p).

- **Remark**. The number x is called the discrete logarithm of h to the base g, denoted $x = \log_g(h)$, or index, $ind_g(h)$.

Diffie-Hellman key exchange

Public Parameter Creation

A trusted party chooses and publishes a (large) prime p and an integer g having large prime order in F_p^*

Private Computations

Alice	Bob
Choose a secret integer a.	Choose a secret integer b.
Compute $A \equiv g^a \pmod{p}$.	Compute $B \equiv g^b \pmod{p}$.

Public Exchange of Values

Alice sends A to Bob $\longrightarrow$	A
B	$\longleftarrow$ Bob sends to Alice

Further Private Computations

Compute the number $K \equiv B^a \pmod{p}$	Compute the number $K \equiv A^b \pmod{p}$

ElGamal public key cryptosystem

It is just a variation of Diffie-Hellman key-exchange protocol for encryption data

Paillier Cryptosystems

- λ = lcm(p-1,q-1); n = pq; g $\in Z_{n}{}^{2}$.
- μ = (L(g^{λ} mod n^2)$^{-1}$ (mod n), where L(u)=(u-1)/n
- Public key: (n, g)
- Private key: (λ,μ)
- Encryption: c = $g^m r^n$ mod n^2.
- Decryption: m = L(c^{λ} mod n^2)μ mod n.

Encrypted computing

- Computing without decryption.
- Using homomorphism property of cryptosystems if they have.
- Let G and H be groups. A function ϕ: G $\rightarrow$ H is called a (group) homomorphism if it satisfies $\phi(g_1 * g_2) = \phi(g_1) \circ \phi(g_2)$, $\forall g_1, g_2 \in G$.

Homomorphism cryptosystems

- RSA: if $c_1=m_1^e$ mod n, $c_2=m_2^e$ mod n. Let $c=c_1c_2=m_1^e m_2^e=(m_1m_2)^e$ mod n, then $c=c_1c_2$ is cipher text of m_1m_2.
- Elgamal: if $(g^{r_1},m_1g^{xr_1})$, $(g^{r_2},m_2g^{xr_2})$. Let $(g^{r_1}g^{r_2},m_1g^{xr_1}m_2g^{xr_2})=(g^{r_1+r_2},m_1m_2g^{x(r_1+r_2)})$.
- Paillier:

  $E(m_1+m_2,\ r_1r_2)$
  $=g^{m_1+m_2}(r_1r_2)^n=(g^{m_1}r_1^n)(g^{m_2}r_2^n)=E(m_1,r_1)E(m_2,r_2)$