Introduction to Cryptology

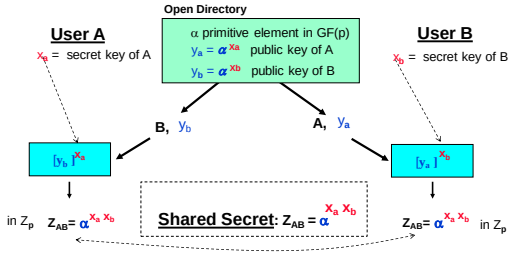
Lecture 13-1- supplementary
Summary of
DH, RSA , ElGamal and Rabin Locks
Most used Crypto-System Locks

17.05.2023, v7

Review
The One-Way Locks
of
DH, RSA, ElGamal, Rabin Locks

1. **Discrete Logarithm Lock**
2. **Factorization Lock**
3. **Elliptic-Curve Algebra**

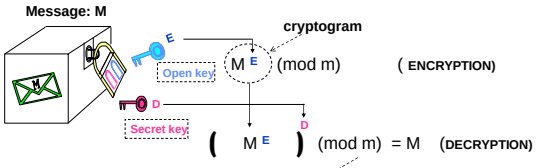
Conventional Diffie-Hellman Public Key Distribution System DH-Lock



Security Claim: log x_a or x_b are not computable from y_a , y_b
(discret log problem is seen as unsolvable)

RSA-Lock (Hiding Function)

Use of Exponentiation in the Ring Z_m where, m = p.q such that p and q are two large secret primes



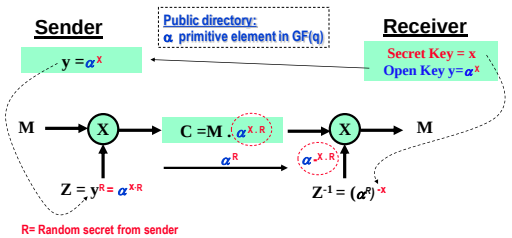
D is the multiplicative inverse of E modulo φ(m)

According to Euler Theorem:
$(M^E)^{D \bmod \varphi(m)} (\text{mod } m) = M^{E \cdot D \bmod \varphi(m)} (\text{mod } m) = M$

Security Claim: φ(m) is only computable if p and q are known!
That is attacker need to factorize m (Factorization problem is unsolvable)

ElGamal Crypto-System 1985

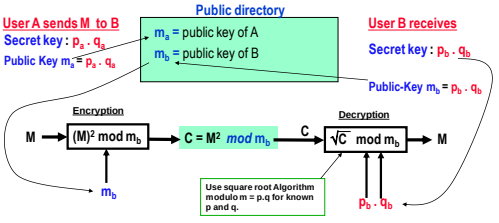
***Basic idea:* Using DH System in a different way**



R= Random secret from sender

Security Claim: same as DH system, (discret log problem is unsolvable)

Rabin Secrecy-System (1979)

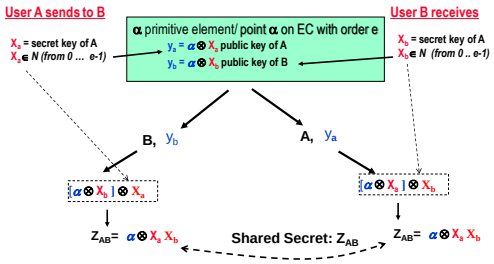


Security Claim: Computing the square root in a ring Z_m is only possible if the ring modulus m is factored (Factorization problem is unsolvable)

Elliptic Curve
Additive Groupe

1. For DH Key-Exchange
2. For ElGamal Crypto

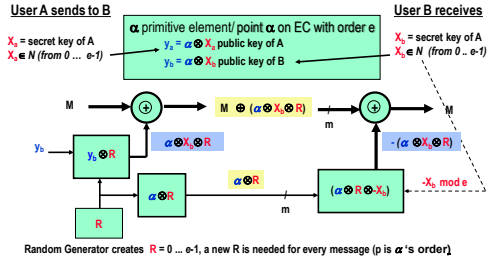
Conventional Diffie-Hellman Public Key Secret-Sharing System Using Additive Groups over Elliptic Curves



El-Gamal Crypto-System
Using Elliptic Curve (EC) Algebra Over GF(2^n) or GF(p)

Neal Koblitz[1] and Victor S. Miller[2] in 1985

System mapping: Substitute addition instead of multiplication and multiplication instead of exponentiation! Same can be done for any discrete log based cryptosystem like Diffie-Helman tec. ..



Random Generator creates R = 0 ... e-1, a new R is needed for every message (p is α 's order)