Public-key Crypptosystems

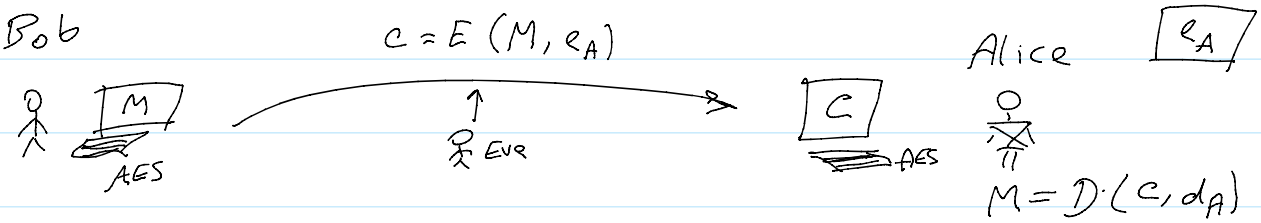
Monday, March 22, 2021 8:38 AM

1] Public-key Crypptosystems (Asymmetric) §10 - Forouzan

* Based on the "hardness" of some math problem §9.1 - Yanofsky

* Each user A has a public-key e_A for encryption and a private-key d_A for decryption

* How it works



* It is computationally infeasible to get d_A from e_A.

2] RSA Cryptosystem:

- 1980's by Rivest, Shamir, Adleman.
- Built on the factorization problem.

3] Setups: for user A

1. Choose large primes: p, q (> 150 digits)
2. $n = p \cdot q \longrightarrow \mathbb{Z}_n^*$ (n is a 300 digits)
3. $\Phi(n) = (p-1)(q-1) = |\mathbb{Z}_n^*|$

4] RSA keys:

- Choose a public-key: e, s.t. $\gcd(e, \Phi(n)) = 1$

  $\Rightarrow$ pub-key: (e, n)

- Compute private-key (using the trap-door: p and q)

$\Rightarrow$ pub-key: (e, n)

- compute private-key (using the trap-door: p and q)

$$d \equiv e^{-1} \pmod{\Phi(n)}$$

5] To encrypt M: $C = E(M, e) = M^e \pmod{n}$

To decrypt C: $D(C, d) = C^d \pmod{n}$

6] RSA Proof: let $M \in \mathbb{Z}_n^*$

$$C \equiv M^e \pmod{n}$$

$$D(C, d) = (M^e)^d \equiv M^{ed} \equiv M^1 \equiv M \pmod{n}$$

7] How the computation is done?

① $d \equiv e^{-1} \pmod{\Phi(n)}$ by EEA

② M^e, C^d by fast modular-exponentiation.

8] e.g. RSA

Setup RSA scheme with $p = 5$, $q = 11$, and find the keys.

① $n = p \cdot q = 5 \cdot 11 = 55$

② $\Phi(n) = 4 \cdot 10 = 40$

③ pub-key: $e = 3$, co-prime to 40,

pri-key: $d = e^{-1} \pmod{\Phi(n)}$

$= 3^{-1} \pmod{40}$

$= 27 \pmod{40}$

$e = 3$ is very common

$3 \cdot 13 \equiv 39 \equiv -1$

$3(-13) \equiv 1$

$-13 \equiv 27 \pmod{40}$

Encrypt $M = 16$

$$E(16, e=3) \equiv 16^3 \pmod{55}$$

$$\equiv 2^{12} \equiv 2^6 \cdot 2^6 \equiv 9 \cdot 9 \equiv 81 \equiv 26 \pmod{55}$$

Decrypt $C = 26$

$$D(26, d=27) = 26^{27} \pmod{55}$$

Decrypt $C = 26$

$$D(26, d=27) \equiv 26^{27} \equiv 16 \pmod{55}$$

9] Discrete-Log Problem:

Given $a \in \mathbb{Z}_p^*$ and b a generator of $\mathbb{Z}_p^*$, for large p. Find x s.t.

$$a \equiv b^x \pmod{p}$$

i.e. $$x \equiv DLog_b(a) \pmod{p}$$

10] e.g. Given $p = 17$, $a = 4$, $b = 3$

find x s.t. $3^x \equiv 4 \pmod{17}$

$\langle 3 \rangle = \{3, 9, 10, 13, 5, 15, 11, 16, \ldots, 0, \ldots, 1\}$

11] Note: It is computationally infeasible to solve DLog.

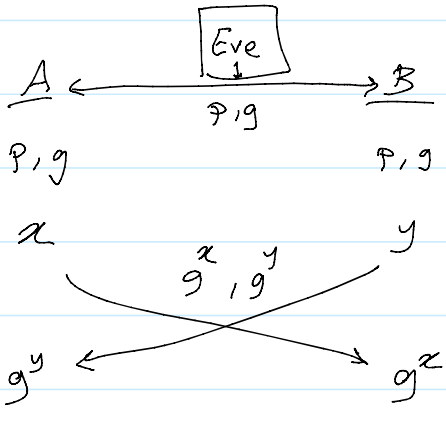
12] Diffie-Hellman Key-Exchange Scheme

1. Alice and Bob agree on p, $\langle g \rangle = \mathbb{Z}_p^*$
2. A chooses a random $x \in \mathbb{Z}_p^*$

   B choose a random $y \in \mathbb{Z}_p^*$
3. A sends g^x to Bob

   B send g^y to Alice
4. A computes: $key = (g^y)^x = g^{xy}$

   B computes: $key = (g^x)^y = g^{xy}$



$$(g^x)^y = g^{xy} = (g^y)^x$$

13] Diffie-Hellman Assumption:

13] Diffie - Hellman Assumption:

"It is computationally infeasible to compute g^{xy} knowing only g^x and g^y"