ICT Course: Introduction to Cryptography

Nguyen Minh Huong

ICT Department, USTH

February 7, 2023

Session 6: Asymmetric Cryptography - RSA Cryptosystem and Diffie-Hellman Key Exchange

Overview of RSA

- be made practical by Rivest, Shamir and Aldeman
- the most widely used asymmetric cryptosystem
- Applications: Transport of (symmetric) keys and Digital Signature

RSA Key Generation

$p=11 \quad q=3$

- Choose 2 large prime numbers p, q: $N = p * q$
- Choose e relative prime to $(p-1)(q-1)$ $= 20$
- Find d:

$$ed = 1 \; mod(p-1)(q-1) \iff e^{-1} \; mod(p-1)(q-1) = d$$

- RSA key pair consists of: $(33, 3)$
  - Public key: (N, e)
  - Private key: d (7)

  where N: modulus, e: encryption exponent, d: decryption exponent
- N has 1024 bits or 2048 bits or larger

Encryption - Decryption

$p = 11 \quad q = 3 \quad M = 15$

pub key : $(33, 3)$

Pri key : 7

- Encryption: $C \equiv M^e (modN)$
- Decryption: $M \equiv C^d (modN)$

$C \equiv 538^3 \bmod 33$

$M = 538 \rightarrow C = 10$

$538^3 \bmod 33 \equiv 10$

$M \equiv 10^7 \bmod 33 = 10$

Proof of correctness

proof that: if $C \equiv M^{e} \bmod N$

$\rightarrow M \equiv C^{d} \bmod N$

Euler's phi function reminds:

- $\phi(m)$ is the number of positive integers less than m that are relatively prime to m
- For any prime number p: $\phi(p) = (p - 1)$
- If p, q are prime: $\phi(p * q) = (p - 1)(q - 1)$

Euler's Theorem

If x is relative prime to n then $x^{\phi(n)} \equiv 1 \; mod \; n$

Proof of correctness

- Assume that M is relatively prime to N, proof the correctness of RSA?
- If M is not prime to N, proof of the correctness of RSA?

Textbook RSA example

- $p = 11$, $q = 3$, choose $e = 3$
- Key pairs?
- Describe the encryption and decryption using RSA if Bob want to send a plaintext $M = 15$ to Alice?

- Example: $(N, e) = (33, 23)$, $M = 5$, Calculate C
- Problem?
- Repeated Squaring method

- Using same exponent e for all users and different p, q are chosen for each key pair
- Common used encryption exponent:
  - $e = 3$: requires $M > N^{1/3}$ to avoid **cube root attack**
  - $e = 2^{16} + 1$

Cryptanalysis

- Protocol attack
- Mathematical attack
- Side-channel attack

Diffie-Hellman Key exchange - Overview[1]

- Proposed in 1976 by Whitfield Diffie and Martin Hellman
- Widely used, e.g. in Secure Shell (SSH), Transport Layer security (TLS), Internet Protocol Security (IPSec)
- Used to establish a shared key, not usually for encryption

[1] Understanding Cryptography by Christof Paar and Jan Pelzl

$g = 3 \qquad p = 17$

group X: $a_x = \ldots$

compute: $g^{a} \bmod p = \underline{A_x}$

Group Y: a_y Receive A_x

Compute: $A_x^{a_y} \bmod p = k_{xy}$

Diffie-Hellman Key Exchange

Discrete Logarithm problem:

Given integers g, p, $g^k\ mod\ p$, find k
$\Longrightarrow$ Very difficult to solve

Diffie-Hellman Key Echange setup:

- Choose a large prime p and a (integer) generator g
- $\forall x \in \{1, 2, ..., p-1\}, \exists n: \ x \equiv g^n(mod\ p)$
- g, p are public

Diffie-Hellman Key Exchange(DHKE)

Alice		Bob
Choose random private key $k_{prA}=a \in \{1,2,\ldots,p-1\}$		Choose random private key $k_{prB}=b \in \{1,2,\ldots,p-1\}$
Compute corresponding public key $k_{pubA}= A = \alpha^a \bmod p$	$\xrightarrow{A}$	
	$\xleftarrow{B}$	Compute correspondig public key $k_{pubB}= B = \alpha^b \bmod p$
Compute common secret $k_{AB} = B^a = (\alpha^a)^b \bmod p$		Compute common secret $k_{AB} = A^b = (\alpha^b)^a \bmod p$

We can now use the joint key k_{AB} for encryption, e.g., with AES

$y = AES_{kAB}(x)$	$\xrightarrow{y}$	$x = AES^{-1}{}_{kAB}(y)$

6/19

Chapter 8 of *Understanding Cryptography* by Christof Paar and Jan Pelzl

DHKE - Man-in-Middle Attack

- Confidentiality:
  - use key pairs to encrypt data
  - hybrid cryptosystem
- Integrity: Digital signature