RSA and Diffie-Hellman Key Exchange

AIF183119 Keamanan Informasi
Universitas Katolik Parahyangan
Mariskha Tri Adithia MSc, PDEng

Overview

- Diffie-Hellman key exchange
- Some math
- Key generation
- Encryption and decryption
- RSA security

Diffie-Hellman Key Exchange

- Key exchange algorithm for symmetric key cryptography
- Exchanging information which is not secret to generate secret key
- Entities should first agree on 2 prime large numbers *n* and *g*, such that $g < n$

The algorithm

Alice		Bob
Generate *x*		Generate *y*
Compute $X = g^x \bmod n$	$\xrightarrow{X}$	
	$\xleftarrow{Y}$	Compute $Y = g^y \bmod n$
Compute symmetric key $K = Y^x \bmod n$		Compute symmetric key $K = X^y \bmod n$

The algorithm

Example

- Misalkan n = 97 dan g = 5
- Alice memilih x = 36, maka

$$X = g^x \bmod n = 5^{36} \bmod 97 = 50$$

- Alice mengirimkan X pada Bob
- Bob memilih y = 58, maka

$$Y = g^y \bmod n = 5^{58} \bmod 97 = 44$$

- Bob mengirimkan Y pada Alice
- Maka kunci simetri yang didapat

$$K = X^y \bmod n = 44^{36} \bmod 97 = 75$$

$$K = Y^x \bmod n = 50^{58} \bmod 97 = 75$$

Exercise

Determine the symmetric key generated by Alice and Bob if $n = 17$ and $g = 3$, $x = 2$, and $y = 5$. Draw the key exchange scheme.

Weaknesses

- Discrete logarithm attack-> computing the value of x and y
  - p should be very big, > 300 digits
  - p-1 should have at least one big prime factors, > 60 digits
  - x and y should be destroyed once the key is generated
- Man-in-the-middle attack
  - How?

Math in RSA

- Greatest Common Divisor (GCD)

  Example:

  Factors of 45: 1,3,5,9,15,45

  Factors of 36: 1,2,3,4,9,12,18,36

  GCD(45,36)=9

Math in RSA (2)

- Relatively prime

  a and b are relatively prime if the GCD(a,b) = 1

  Examples:

  23 and 13, and 125 and 4, are relatively prime

Key generation

No.	Variables	Properties
1	*Prime numbers p* and *q*	Secret
2	$n = p \cdot q$	Public
3	$\phi(n) = (p-1)(q-1)$	Secret
4	*e* (encryption key)	Public
5	*d* (decryption key)	Secret
6	*m* (plaintext)	Secret
7	*c* (ciphertext)	Public

Key generation (2)

1. Choose two prime numbers p and q
2. Compute $n = p \cdot q$ ($p \neq q$, why?)
3. Compute $\phi(n) = (p-1)(q-1)$
4. Choose a public key e, which is relatively prime with $\phi(n)$
5. Generate the private key, $d = e^{-1} \bmod \phi(n)$

Kunci publik adalah pasangan (e,n)
Kunci privat adalah d

Key generation (3)

Example:

1. Suppose $p = 47$ and $q = 71$
2. Compute $n = p \cdot q = 47 \cdot 71 = 3337$
3. Determine $\phi(n) = (p-1)(q-1) = 46 \cdot 70 = 3220$
4. Suppose the public key $e = 79$
5. Generate the private key $d = 79^{-1} \bmod 3220 = 1019$

Exercise

Determine the public and private keys if $p = 53$ and $q = 67$.

Encryption and decryption

Encryption algorithm

1. Suppose the receiver public key and modulus are *e* and *n*, respectively
2. Divide the plaintext *m* into blocks $m_1, m_2, \ldots$ such that $m_1, m_2, \ldots$ in $[0, n-1]$
3. Encrypt block m_i as $c_i = m_i^e \bmod n$

Decryption algorithm

Decrypt ciphertext c_i as $m_i = c_i^d \bmod n$

Encryption and decryption Example

- Alice wants to send a message to Bob
- Alice’s message is m = HARI INI or m = 7265827332737873 in ASCII code, n = 3337
- Divide m into blocks of 3 digits (why?)

$$
\begin{aligned}
m_1 &= 726 \qquad & m_4 &= 273 \\
m_2 &= 582 \qquad & m_5 &= 787 \\
m_3 &= 733 \qquad & m_6 &= 003
\end{aligned}
$$

Encryption and decryption Example (2)

- Encrypt m using Bob's public key e = 79 as follows:

$$m_1 = 726^{79} \bmod 3337 = 215$$
$$m_2 = 582^{79} \bmod 3337 = 1743$$
$$m_3 = 733^{79} \bmod 3337 = 1731$$

$$m_4 = 273^{79} \bmod 3337 = 776$$
$$m_5 = 787^{79} \bmod 3337 = 933$$
$$m_6 = 003^{79} \bmod 3337 = 158$$

- The ciphertext is

  c = 215 1743 1731 776 933 158

Encryption and decryption
Example (3)

- Bob decrypts the message using his private key d = 1019, as follows:

$$m_1 = 215^{1019} \bmod 3337 = 726$$
$$m_4 = 776^{1019} \bmod 3337 = 582$$
$$m_2 = 1743^{1019} \bmod 3337 = 733$$

$$m_5 = 933^{1019} \bmod 3337 = 273$$
$$m_3 = 1731^{1019} \bmod 3337 = 787$$
$$m_6 = 158^{1019} \bmod 3337 = 3$$

Exercise

Determine the public and private keys given $p = 3$ and $q = 7$ and encrypt the message $m = 1214200915$

Discussion

- If you want to attack the RSA, what will you do?

Questions?