Chapter Three

Asymmetric Cryptosystem

Public Key Cryptography

The concept of asymmetric or public key cryptography was invented by Diffie-Hellman in 1976. Their paper titled " New directions in Cryptography" was published in IEEE transaction In information theory, vol. 22, no. 6, November 1976, pp. 644-654. Their paper was cited by 14669 related articles (information accessed on 28 July 2016). Diffie-Hellman received Turing award in 2015 for their contribution in cryptography.

Merkle-Hellman Cryptosystem

Merkle-Hellman Knapsack cryptosystem is an asymmetric or public key cryptosystem invented in 1978.

This cryptosystem includes key generating, encryption and decryption processes.

Key generation:

a) Private key:

Sub Set	Sum of sub-set	Next Integer
2	2	3
2, 3	5	7
2, 3, 7	12	13
2, 3, 7, 13	25	27

Key generation

S = (2, 3, 7, 13) is selected as secret or private key.

b) Public key:

public key is computed using the following equation:

$$p_i = e^*s_i \bmod n \qquad (1)$$

Select *e* and *n* such that $e < n$ and $gcd(e, n) = 1$, *e.i.*, *e* and *n* are relatively primes. Such as, Choose $e = 25$ and $n = 29$.

Key generation [cont..]

We have S = (2, 3, 7, 13), e = 25, n = 29.

p_1 = 2 * 25 mod 29 = 21
p_2 = 3 * 25 mod 29 = 17
p_3 = 7 * 25 mod 29 = 01
p_4 = 13 * 25 mod 29 = 06

P = (21, 17, 1, 6) is the public key.

Encryption process

To do encryption the message is divided into blocks.

Encryption can be done using the following equation:

$$c_j = \sum_{i=1}^{k} b_i \, p_i \quad for \, 1 \le j \le m$$

where *k* is the number of bits in a block and there are *m* blocks in a message.

Encryption [Cont..]

Suppose we have a message and its binary form is as follows:

$$M = 10011011010111010011$$

Divide the message into blocks

$$M = 1001 \quad 1011 \quad 0101 \quad 1101 \quad 0011$$

$$P = (21, 17, 1, 6)$$

$c_1 = 1 * 21 + 0 * 17 + 0 * 1 + 1 * 6 = 27$

$c_2 = 1 * 21 + 0 * 17 + 1 * 1 + 1 * 6 = 28$

$c_3 = 0 * 21 + 1 * 17 + 0 * 1 + 1 * 6 = 23$

Encryption [Cont..]

$c_4 = 1 * 21 + 1 * 17 + 0 * 1 + 1 * 6 = 44$

$c_5 = 0 * 21 + 0 * 17 + 1 * 1 + 1 * 6 = 7$

The cipher text is then,

C = (27, 28, 23, 44, 7).

Without knowing the private key it is very difficult to find the original message.

Decryption process

Decryption can be done using the following equation:

$$\sum_{i=1}^{k} s_i b_i = c_j \, x \bmod n \quad for\, 1 \le j \le m \qquad (3)$$

where *x* = M-inv (e, n), M-inv denotes multiplicative inverse, which means

e*x mod n = 1 (4)

We have e = 25 and n = 29, from the equation (4) we get

x = 7 or M-inv (25, 29) = 7.

We can find M-inv of any two numbers using **Extended Euclidian algorithm**. We study it later.

Decryption [cont..]

We have C = (27, 28, 23, 44, 7)

According to the right side of the equation (3)

$c_1 * x \bmod n = 27 * 7 \bmod 29 = 15$

$c_2 * x \bmod n = 28 * 7 \bmod 29 = 22$

$c_3 * x \bmod n = 23 * 7 \bmod 29 = 16$

$c_4 * x \bmod n = 44 * 7 \bmod 29 = 18$

$c_5 * x \bmod n = 7 * 7 \bmod 29 = 20$

Decryption [cont..]

According to the equation (3)

[2, 3, 7, 13] * [1 0 0 1] = 15

[2, 3, 7, 13] * [1 0 1 1] = 22

[2, 3, 7, 13] * [0 1 0 1] = 16

[2, 3, 7, 13] * [1 1 0 1] = 18

[2, 3, 7, 13] * [0 0 1 1] = 20

The original message is then:

1001 1011 0101 1101 0011

RSA Cryptosystem

This cryptosystem is invented by Rivest, Shamir and Adleman (RSA) in 1979.

It is a public key cryptosystem, which involves exponentiation modulo a number, n that is a product of two large prime numbers.

The 1024 bits key size is a typical key size for RSA cryptosystem.

Key Generation Process

1. Select at random two large prime numbers ***p*** and ***q***.

   (The primes *p* and *q* might be, say, **100 decimal digits each.**)
2. Compute ***n*** by the equation $n = pq$.

3. Select a small odd integer ***e*** that is relatively prime to **m**, where
   $m = (p - 1)(q - 1)$.

4. Compute ***d*** as the multiplicative inverse of ***e***, modulo **m** , *i.e.*,
   $e*d \bmod m = 1$ or d = minv (*e*, m) here gcd(e, m)=1.

5. Publish the pair $p = (e, n)$ as RSA public key.

6. Keep secret the pair $s = (d, n)$ as RSA secret key.

Encryption and Decryption

Encryption Process: The transformation of a message M associated with a public key $p = (e, n)$, is as follows:

$$C = E(M) = M^e \pmod{n}.$$

Decryption Process: The transformation of a cipher text C associated with a secret key $S = (d, n)$ is as follows:

$$M = D(C) = C^d \pmod{n}.$$

MULTIPLICATIVE INVERSES

Given an integer *a* in the range [0, *n*-1], it may be possible a unique integer *x* in the range [0, *n*-1] such that

$$ax \bmod m = 1.$$

Here ***a*** and ***x*** are multiplicative inverses mod ***n***. For example, 3 and 7 are multiplicative inverses mod 10, because 21 mod 10 = 1.

$$ax \bmod m = 1 \qquad (1)$$

$$ax \equiv 1 \pmod{m} \qquad (2)$$

$$x = \mathrm{minv}\,(a, m) \qquad (3)$$

(1) and (2) are equivalent expressions. We can find multi-plicative inverse (minv) using **Extended Euclid's a**lgorithm

Extended Euclid's Algorithm:

// Given two positive integers m and *p*, we compute *gcd* *d* and two integers.
//*a* and *b*, such that $am + bp = d$

1. set $a \leftarrow 0$, $a' \leftarrow 1$, $c \leftarrow m$; $b \leftarrow 1$, $b' \leftarrow 0$, $d \leftarrow p$;
2. $q \leftarrow$ quotient $(c \div d)$; $r \leftarrow$ remainder $(c \div d)$;
3. If $r = 0$, the algorithm terminates; and $am + bp = d$ as described.
4. set $c \leftarrow d$, $d \leftarrow r$; $t \leftarrow a'$, $a' \leftarrow a$, $a \leftarrow t - qa$;

   $t \leftarrow b'$, $b' \leftarrow b$, $b \leftarrow t - qb$; and go back to step 2.

If from above algorithm $b \geq 0$, minv = b, otherwise minv = b + m

Example of minv calculation

dx mod c = 1, *x* = minv (d, c)
d = 83, c = 4620

	Sl#	*b'*	*b*	*c*	*d*	*r*	*q*
	1	**0**	**1**	4620	83	55	**55**
	2	1	-55	83	55	28	1
	3	-55	56	55	28	27	1
	4	56	-111	28	27	1	1
	5	-111	**167**	27	1	0	27

From 1st Row: *b*' = 0, b = 1, q = 55

Calculation For 2nd row:

$t \leftarrow b'$, $b' \leftarrow b$ $b \leftarrow t - qb$;

t = 0, b' = 1, b = 0 – 55*1 = -55,

Calculation for b

From 2nd Row: $b' = 1$, $b = -55$, $q = 1$

Calculation For 3nd row:

$t \leftarrow b'$, $\quad b \leftarrow t - qb;$

$t = 1$, $\quad b = 1 - (-55*1) = 56$,

From 3rd row: $b' = -55$, $q = 1$, $b = 56$

Calculation for 4th row:

$b = t - q*b = -55 - (1*-56) = -55 - 56 = -111$

Another Example

$dx \bmod c = 1$, $x = \text{minv}(d, c)$

$d = 23$, $c = 280$

	Sl#	b'	b	c	d	r	q
	1	**0**	**1**	280	23	4	12
	2	1	-12	23	4	3	5
	3	-12	61	4	3	1	1
	4	61	-73	3	1	**0**	3

From 1st Row: b' = 0, q = 12, b = 1

Calculation For 2nd row:

$t \leftarrow b'$, $b \leftarrow t - qb$;

t = 0, b = 0 – 12*1 = -12,

Calculation for b

From 2nd Row: *b'* = 1, q = 5, b = -12

Calculation For 3nd row:

$t \leftarrow b'$, $b \leftarrow t - qb$;

t = 1, b = 1 – (-12*5) = 61,

Calculation for 4th row:

t =-12,

b =t - q*b = -12 - (1*61) = -73

If b < 0, b = b + c =-73 + 280 = 207

So, M-inv (23, 280) = 207

MODULAR EXPONENTIATION

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

1. C: = M (mod n)
2. for $i = e-1$ down to 1
3. C: = C. M (mod n)
4. return C

Example: M = 7, e = 5 and n = 11

$M^e \pmod{n} = 7^5 \pmod{11}$

1) C = 7 mod 11 = 7 $\rightarrow$ M (mod n)
2) C = 7.7 mod 11 = 5 $\rightarrow$ $M^2 \pmod{n}$
3) C = 5.7 mod 11 = 2 $\rightarrow$ $M^3 \pmod{n}$
4) C = 2.7 mod 11 = 3 $\rightarrow$ $M^4 \pmod{n}$
5) C = 3.7 mod 11 = 10 $\rightarrow$ $M^5 \pmod{n}$

Example of RSA cryptosystem

1. *Take* p = 67 and q = 71
2. *Compute* $n = p*q$ = 67*71 = 4757
3. *Compute* $m = \varphi(n) = (p-1)(q-1)$ = 66*70 = 4620
4. Choose e = **83**, such that gcd(e, m) = 1.
5. *Compute* d = m-inv(**83**, 4620) = 167
6. Public key is (e, n) = (83, 4757)
7. Secret key is (d, n) = (167, 4757)

Example of RSA [cont..]

Take a message: CONFIDENTIAL

Message is encoded (letter to digit) as follows:

blank = 00, A = 01, B = 02 and so on.

C	O	N	F	I	D	E	N	T	I	A	L
03	15	14	06	09	04	05	14	20	09	01	12

By taking two letter as a block, we get following data:

0315 1406 0904 0514 2009 0112

Here we must consider that the value of each block must be less than the value of *n*.

So, $M = (m_1, m_2, m_3, m_4, m_5, m_6) = (315, 1406, 904, 524, 2009, 112)$

Example of RSA [cont..]

Encryption process:

Encrypt the message as, $C = M^e \bmod n$

$C_1 = m_1^e \bmod n = 315^{83} \bmod 4757 = 4461$

$C_2 = 1406^{83} \bmod 4757 = 1942$

$C_3 = 904^{83} \bmod 4757 = 4231$

$C_4 = 514^{83} \bmod 4757 = 511$

$C_5 = 2009^{83} \bmod 4757 = 4622$

$C_6 = 112^{83} \bmod 4757 = 310$

Cipher text C = (4461, 1942, 4231, 511, 4622, 310)

Example of RSA [cont..]

Decryption Process:

Decrypt the cipher text as, $M = c^{d} \bmod n$

$m_1 = C_1^d \bmod n = 4461^{167} \bmod 4757 = 315$

$m_2 = 1942^{167} \bmod 4757 = 1406$

$m_3 = 4231^{167} \bmod 4757 = 904$

$m_4 = 514^{167} \bmod 4757 = 514$

$m_5 = 4622^{167} \bmod 4757 = 2009$

$m_6 = 310^{167} \bmod 4757 = 112$

The original message M = (315 1406 904 514 2009 112)

Example of RSA [cont..]

By decoding the number to letter we get the original message as follows:

315 = CO, 1406 = NF, 904 = ID, 514 = EN,
2009 = TI, 112 = AL

Then we get the message: **CONFIDENTIAL**

This is the end

of

Asymmetric Cryptosystem.

Thank You.