CHAPTER 4
PUBLIC KEY CRYPTO

PREPARED BY:

DR. MUHAMMAD IQBAL HOSSAIN

ASSOCIATE PROFESSOR

DEPARTMENT OF CSE, BRAC UNIVERSITY

APPENDIX

MODULAR ARITHMETIC

KNAPSACK

RSA

DIFFIE-HELLMAN KEY EXCHANGE

ELLIPTIC CURVE CRYPTOGRAPHY

USES FOR PUBLIC KEY CRYPTO

MODULAR ARITHMETIC

- For integer x and n, "x mod n" is the remainder of x / n.
- Examples

7 mod 6 = 1

33 mod 5 = 3

33 mod 6=3

51 mod 17 = 0

17 mod 6 = 5

<u>Practice</u>

6 mod 5 = ?

23 mod 5 = ?

10 mod 5 = ?

58 mod 20 = ?

100 mod 20 = ?

MODULAR ADDITION

- **Notation and facts**
  - 7 mod 6 = 1
  - 7 = 13 = 1 mod 6
  - ((a mod n) + (b mod n)) mod n = (a + b) mod n
  - ((a mod n)(b mod n)) mod n = ad mod n
- **Addition example**
  - 3 + 5 = 2 mod 6
  - 2 + 4 = 0 mod 6
  - 3 + 3 = 0 mod 6
  - (7 + 12) mod 6 = 19 mod 6 = 1 mod 6
  - (7 + 12) mod 6 = (1 + 0) mod 6 = 1 mod 6

MODULAR MULTIPLICATION

- **Multiplication example**
  - 3 . 4 = 0 mod 6
  - 2 . 4 = 2 mod 6
  - 5 . 5 = 1 mod 6
  - (7 . 4) mod 6 = 28 mod 6 = 4 mod 6
  - (7 .4) mod 6 = (1 .4) mod 6 = 4 mod 6

MODULAR INVERSE

- *Additive inverse* of x mod n, denoted as –x mod n, is the number that must be added to x to get 0 mod n.
  - -2 mod 4 = 6 since 2+4 = 0+6
- *Multiplicative inverse* of x mod n, denoted x^{-1} mod n, in the number that must be multiplicative by x to get 1 mod n.
  - 3^{-1} mod 7 = 5; since 3.5 = 1 mod 7

MODULAR ARITHMETIC QUIZ

- What is -3 mod 6?
- 3

3+3 mod 6 = 0

- What is -1 mod 6?
- 5

1+5 = 0 mod 6

- What is 5^{-1} mod 6?
- 5

5*5 mod 6 = 0
or, 5*5 = 0 mod 6

- What is 2^{-1} mod 6?
- ???

RELATIVE PRIMALITY

- x and y are relatively prime if they have no common factor other than 1.
- x^{-1} mod y exists only when x and y are relatively
- prime.
- x^{-1} mod y is easy to find (when it exits) using **Euclidean** algorithm

TOTIENT FUNCTION

- $\phi(n)$ in the number of numbers less than n that are relatively prime to n.
  - Positive integer.
- Example
  - $\phi(4) = 2$ since 4 is relatively prime to 3, 1.
  - $\phi(5) = 4$ since 5 is relatively prime to 1, 2, 3, 4
  - $\phi(12) = 4$
  - $\phi(p) = p-1$ if p in prime.
  - $\phi(pq) = (p-1)(q-1)$ if p and q prime

$\mathbb{Z}_{26} = (0, 1, 2 \ldots 25)$

od 26

tion

$\boxed{Gcd(973, 301) = ??}$

$\boxed{11^{-1} \bmod 26 = 19}$

$t = t_i - g\, t_{i+1}$

g	r_1	r_2	r	t_1	t_2	t
2	26	11	4	0	1	-2
2	11	4	3	1	-2	5
1	4	3	1	-2	5	-7
3	3	1	0	5	-7	26

$0 - 2 \cdot 1 = -2$

$1 - (2 \times -2) = 5$

$-2 - (1 \times 5)$

$5 - (3 \times -7)$

$= 26$

$11^{-1} \bmod 26 = -7$

$= -7 + 26$

$= 19$

* $17^{-1} \bmod 203$

$GCD(17, 203) = 1$

17 | 203 | 11
17
33
17
16

16 | 17 | 1
16
1

1 | 16 | 16
16
X

2 | 16 | 8
16
0

q	r_1	r_2	r	t_1	t_2	t
11	203	17	16	0	1	-11
1	17	16	1	1	-11	$\boxed{12}$
16	16	1	0	-11	12	

$t = t_i - q\,t_{i+1}$

$t = 0 - 11 \times 1$
$= -11$

$1 - (1 \times -11)$
$1 + 11$
$= 12$

$\boxed{71^{-1} \bmod 181}$

11^{-1} mod

*

$\boxed{11^{-1} \bmod 26} = ?\ -7 + 26$

$= 19$

$\gcd(11, 26) = 1$

q	r_1	r_2	r	t_1	t_2	t
2	26	11	4	0	1	-2
2	11	4	3	1	-2	5
1	4	3	1	-2	5	-7
3	3	1	$\boxed{0}$	5	$\boxed{-7}$	26

$11^{-1} \bmod 26 = -7 + 26$

$= 19$

$11 \overline{)26} 2$, 22, 4

$4 \overline{)11} 2$, 8, 3

$3 \overline{)4} 1$, 3, 1

$1 \overline{)3} 3$, 3, 0

$t = t_i - q t_{i+1}$

$t = t_1 - q t_2$

$= 0 - (2 \times 1)$

$= -2$

$1 - (2 \times -2)$

$t = -2 - (1 \times 5)$

$= -7$

$t = 5 - (3 \times (-7))$

$= 26$

PKC IS NEWCOMER

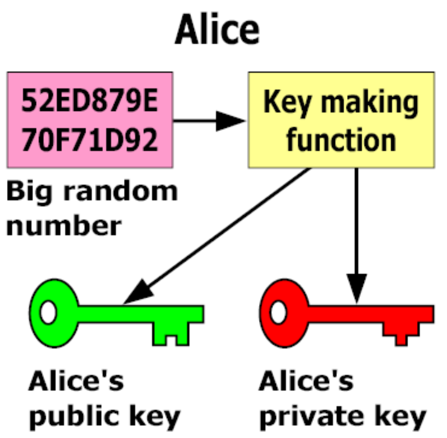
- Different name
  - Asymmetric cryptography
    - Consider the symmetric cryptography
  - Two key cryptography
  - Non-security key cryptography
- The concept is relative newcomer
  - In the late 1960s by GCHQ of British
  - Independently, in early 1970s by academic researchers

MISCONCEPTIONS ON PKC

- PKC is more secure than that of symm cipher
  - Cipher Security is depends on computational work to break a cipher – both are depends on it
- PKC made symm cipher obsolete
  - The problem of computation overhead of PKC
- Key distribution of PKC is trivial
  - The procedures of PKC are so not simpler and more efficient than those of symm cipher
  - PKI is required for the key distribution of PKC

KEY GENERATION OF PKC

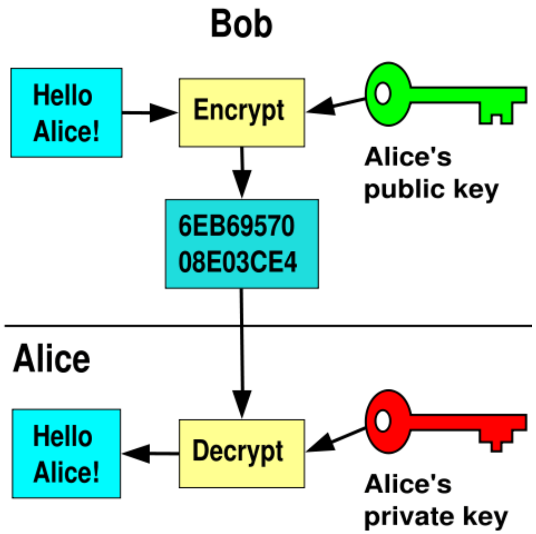
- Making two keys: Based on **trap door one way function**
  - Easy to compute in one direction
  - Hard to compute in other direction
  - "Trap door" used to create keys
  - Example: Given **p** and **q**, product **N=pq** is easy to compute, but given **N**, it is hard to find **p** and **q**



- A message encrypted by the public key can decrypted only with the corresponding private key

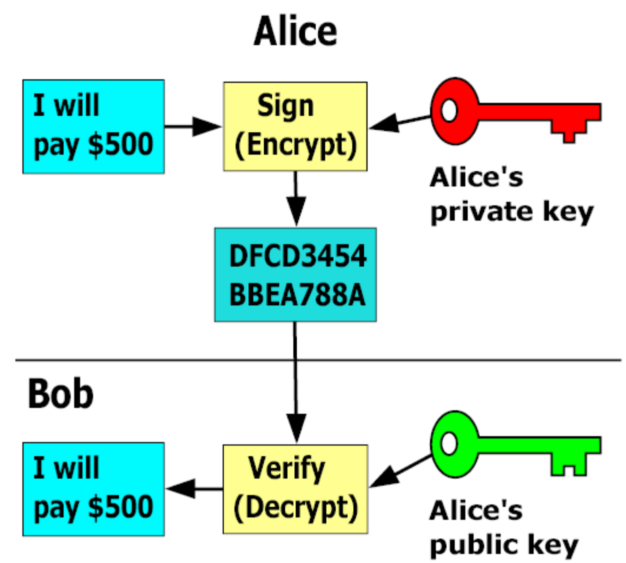
TWO MAIN BRACHES OF PKC

- Public key Encryption
  - Suppose we encrypt **M** with Alice’s public key
  - Only Alice’s private key can decrypt to find **M**



TWO MAIN BRANCHES OF PKC

- Digital Signature
  - Sign by "encrypting" with private key
  - Anyone can **verify** signature by "decrypting" with public key



- But only private key holder could have signed
- Like a handwritten signature (and then some)

PKCS TO DISCUSS

- Knanpsack
  - The first proposed PKC
  - It is inscure
- RSA
  - Problem of factoring large numbers
- Diffie-Hellman Key Exchange
  - Discrete log problem
- ECC(Elliptic Curve Cryptography)
  - Based on the algebraic structure of elliptic curves over finite fields

KNAPSACK

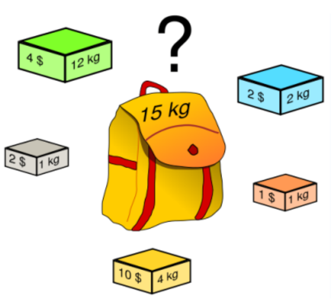
KNAPSACK PROBLEM

- Given a set of n weights $W_0, W_1, \cdots W_{n-1}$ and a sum S, is it possible to find $a_i \in \{0,1\}$ so that

$$S = a_0 W_0 + a_1 W_1, \cdots + a_{n-1} W_{n-1}$$

(technically, this is "subset sum" problem)

- Example
  - Weights (62,93,26,52,166,48,91,141)
  - Problem: Find subset that sums to S=302
  - Answer: 62+26+166+48=302
- The (general) knapsack is NP-complete



KNAPSACK PROBLEM

- General knapsack (GK) is hard to solve
- But superincreasing knapsack (SIK) is easy
- SIK each weight greater than the sum of all previous weights
- Example
  - Weights (2,3,7,14,30,57,120,251)
  - Problem: Find subset that sums to S=186
  - Work from largest to smallest weight
  - Answer: 120+57+7+2=186

KNAPSACK CRYPTOSYSTEM

1. Generate superincreasing knapsack (SIK)
2. Convert SIK into "general" knapsack (GK)
   - Public Key: **GK**
   - Private Key: **SIK plus conversion factors**

- Easy to encrypt with GK
- With private key, easy to decrypt (convert ciphertext to SIK)
- Without private key, must solve GK (???)

KNAPSACK CRYPTOSYSTEM

1. Let (2,3,7,14,30,57,120,251) be the SIK
2. Choose **m** = 41 and **n** = 491 with **m**, **n** rel. prime and **n** greater than sum of elements of SIK

   Then General knapsack can be computed;

3. General knapsack: (82,123,287,83,248,373,10,471)

$$
\begin{aligned}
2 \cdot 41 \bmod 491 &= 82 \\
3 \cdot 41 \bmod 491 &= 123 \\
7 \cdot 41 \bmod 491 &= 287 \\
14 \cdot 41 \bmod 491 &= 83 \\
30 \cdot 41 \bmod 491 &= 248 \\
57 \cdot 41 \bmod 491 &= 373 \\
120 \cdot 41 \bmod 491 &= 10 \\
252 \cdot 41 \bmod 491 &= 471
\end{aligned}
$$

KNAPSACK EXAMPLE

- Private key: **(2,3,7,14,30,57,120,251)**

$$n = 491 \qquad m^{-1} \bmod n \;\rightarrow\; 41^{-1} \bmod 491 = 12$$

- Public key: **(82,123,287,83,248,373,10,471)**
- Example: Encrypt 10010110

  82 + 83 + 373 + 10 = 548

- To decrypt
  - 548 · 12 = 193 mod 491 = S
  - Solve (easy) SIK with S = 193
  - 193=2+14+57+120
  - Obtain plaintext 10010110

$$\begin{aligned}
2 \cdot 41 \bmod 491 &= 82 \\
3 \cdot 41 \bmod 491 &= 123 \\
7 \cdot 41 \bmod 491 &= 287 \\
14 \cdot 41 \bmod 491 &= 83 \\
30 \cdot 41 \bmod 491 &= 248 \\
57 \cdot 41 \bmod 491 &= 373 \\
120 \cdot 41 \bmod 491 &= 10 \\
252 \cdot 41 \bmod 491 &= 471
\end{aligned}$$

KNAPSACK WEAKNESS

- Trapdoor: Convert SIK into “general” knapsack using modular arithmetic
- One-way: General knapsack easy to encrypt, hard to solve; SIK easy to solve
- This knapsack cryptosystem is **insecure**
  - Broken in 1983 with Apple II computer
  - The attack uses **lattice reduction**
  - “General knapsack” derived from SIK is not general enough!
  - This special knapsack is easy to solve!

RSA

- The most difficult computation?

Addition	Multiplication	Factorization
Easy		Difficult
123 + 654 -------- 777	123 x 654 --------- 492 615 738 ----------- 80442	221 = ?x? 221/2 = 221/3 = 221/5 = 221/7 = 221/11 = 221/13 = 221 = 13 x 17

RSA

- Invented by Cocks (GCHQ), independently, by **Rivest**, **Shamir** and **Adleman** (MIT)
- Let p and q be two large prime numbers
- Let $\mathbf{N = pq}$ be the **modulus**
- Choose **e** relatively prime to **(p-1)(q-1)**
- Find **d** s.t. $ed = 1 \bmod (p-1)(q-1)$
- **Public key** is **(N,e)**
- **Private key** is **d**

RSA

- To encrypt message **M** compute
  - $C = M^e \bmod N$
- To decrypt **C** compute
  - $M = C^d \bmod N$
- Recall that **e** and **N** are public
- If attacker can factor **N**, he can use **e** to easily find **d** since ***ed* = *1* mod *(p–1)(q–1)***
- **Factoring the modulus breaks RSA**
- It is not known whether factoring is the only way to break RSA

DOES RSA REALLY WORK?

- Given $C = M^e \bmod N$, we must show

$$M = C^d \bmod N = M^{ed} \bmod N \quad \text{where } M < N$$

- **Euler's Theorem**

If M is relatively prime to N then

$$M^{\phi(N)} = 1 \bmod N \qquad \text{where } \varphi(N) \text{ is totient function}$$

- Facts:
  - $ed = 1 \bmod (p\text{-}1)(q\text{-}1)$
  - By definition of "mod", $ed = k(p-1)(q-1) + 1$

DOES RSA REALLY WORK?

- Facts:
  - $ed = 1 \bmod (p\text{-}1)(q\text{-}1)$ $\quad ed = k(p-1)(q-1)+1$
  - By definition of "mod",
  - $\phi(N) = (p-1)(q-1)$
  - Then $\quad ed - 1 = k(p-1)(q-1) = k\phi(N)$
- Prove

$$
\begin{aligned}
M^{ed} &= M^{(ed-1)+1} = M \bullet M^{ed-1} = M \bullet M^{k\phi(N)} \\
&= M \bullet (M^{\phi(N)})^k \bmod N = M \bullet (1)^k \bmod N \\
&= M \bmod N
\end{aligned}
$$

SIMPLE RSA EXAMPLE

- Example of RSA
  - Select "large" primes $p = 11$, $q = 3$
  - Then $N = pq = 33$ and $(p-1)(q-1) = 20$
  - Choose $e = 3$ (relatively prime to 20)
  - Find d such that $ed = 1 \bmod 20$, we find that $d = 7$ works
- **Public key:** $(N, e) = (33, 3)$
- **Private key:** $d = 7$

SIMPLE RSA EXAMPLE

- **Public key:** (N, e) = (33, 3)
- **Private key:** d = 7
- Suppose message M = 8
- Ciphertext C is computed as

$$C = M^e \bmod N = 8^3 = 512 = 17 \bmod 33$$

- Decrypt C to recover the message M by

$$M = C^d \bmod N = 17^7 = 410{,}338{,}673 \bmod 33$$
$$= 12{,}434{,}505 \times 33 + 8 = 8 \bmod 33$$

MORE EFFICIENT RSA (1)

- Modular exponentiation example
  - $5^{20} = 95367431640625 = 25 \bmod 35$
- A better way: **repeated squaring**
  - $20 = 10100$ base 2
  - $(1, 10, 101, 1010, 10100) = (1, 2, 5, 10, 20)$
  - Note that $2 = 1\cdot 2$, $5 = 2 \cdot 2 + 1$, $10 = 2 \cdot 5$, $20 = 2 \cdot 10$
  - $5^1 = 5 \bmod 35$
  - $5^2 = (5^1)^2 = 5^2 = 25 \bmod 35$
  - $5^5 = (5^2)^2 \cdot 5^1 = 25^2 \cdot 5 = 3125 = 10 \bmod 35$
  - $5^{10} = (5^5)^2 = 10^2 = 100 = 30 \bmod 35$
  - $5^{20} = (5^{10})^2 = 30^2 = 900 = 25 \bmod 35$
- Never have to deal with huge numbers!

MORE EFFICIENT RSA (2)

- Let **e = 3** for all users (but not same N or d)
  - Public key operations only require 2 multiplies
  - Private key operations remain "expensive"
  - If $M < N^{1/3}$ then $C = M^e = M^3$ and **cube root attack**
    - (mod N) operation has no effect
  - For any M, if C_1, C_2, C_3 sent to 3 users, cube root attack works (**uses Chinese Remainder Theorem**)
  - Can prevent cube root attack by padding message with random bits
- Note: $e = 2^{16} + 1$ also used: Protect CRT attack