VASIREDDY VENKATADRI INSTITUTE OF TECHNOLOGY

COURSE NAME: CRYPTOGRAPHY AND NETWORK SECURITY
COURSE CODE: R1641051
COURSE INSTRUCTOR: MADHU BABU JANJANAM, ASSOC. PROF, CSE
UNIT: 3

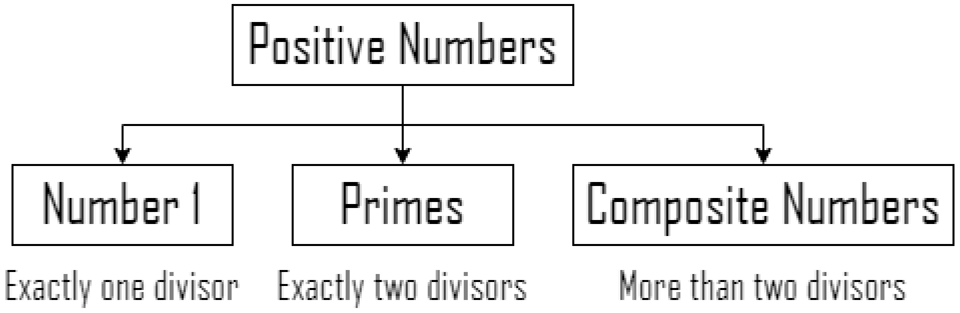
By the end of this unit…

- Explain the mathematics behind Asymmetric Cryptography and working of Asymmetric Cryptographic algorithms.

By the end of this session…

- Define prime numbers and explain their applications in cryptography.

Positive Integers



- Divided into three categories
  - Number with one divisor
  - Numbers with two divisors
  - Numbers with more than two divisors
- A prime number is divisible only by 1 and itself.
- A composite number is divisible by more than two numbers.
- Two positive integers, a and b, are relatively prime, or coprime, if gcd(a,b) = 1.
- Members in Z_n^* are coprimes with number n.
- Members in Z_p^* are coprimes with prime p.

Euler's phi-Function

$$Z_{10}^{*} = \{1,3,7,9\}$$

$$\emptyset(10) = 4$$

$$Z_{7}^{*} = \{1,2,3,4,5,6\}$$

$$\emptyset(7) = 6$$

- Euler's phi-function, $\emptyset(\mathrm{n})$, finds the number of integers that are both smaller than n and relatively prime to n.
- Recall set Z_n^{*}, which contains all the integers which are less than n and relatively prime to n.
- So, $\emptyset(\mathrm{n})$ represents number of integers in Z_n^{*}.
- Also called as Euler's totient function.

Finding the value of $\emptyset(n)$

$1.\ \emptyset(1) = 0$

$2.\ \emptyset(p) = p - 1, if\ p\ is\ a\ prime$

$3.\ \emptyset(m \times n) = \ \emptyset(m) \times \emptyset(n), if\ m\ and\ n\ are\ relatively\ prime$

$4.\ \emptyset(p^e) = \ p^e - \ p^{e-1}, if\ p\ is\ a\ prime$

$Ex: Find\ the\ value\ of\ \emptyset(240)$

$Sol:\ 240 = \ 2^4 \times 3^1 \times 5^1$

$$\emptyset(240) = \ \emptyset(2^4) \times \emptyset(3^1) \times \emptyset(5^1) = (2^4 - 2^3) \times (3^1 - 3^0) \times (5^1 - 5^0)$$

$$= 8 \times 2 \times 4 = 64$$

Finding the value of $\emptyset(n)$ (Contd…)

$Ex: Find\ the\ value\ of\ \emptyset(49)$

$Sol: 49 = \cancel{\emptyset(7) \times \emptyset(7) = 36}$

$= \emptyset(7^2) = 7^2 - 7^1 = 42$

$Conditions\ apply:$

$The\ difficulty\ in\ finding\ \emptyset(n)\ depends\ on\ the\ difficulty\ of\ finding\ the\ factorization\ of\ n.$

Fermat's Little Theorem

$Ex: Find\ the\ result\ of\ 6^{10}\ mod\ 11.$

$Sol:\ 6^{10}\ mod\ 11 = 1$

$Ex: Find\ the\ result\ of\ 3^{12}\ mod\ 11.$

$Sol: 3^{12}\ mod\ 11 = (3^2 \times 3^{10})\ mod\ 11$

$= 3^2\ mod\ 11\ \times\ 3^{10} mod\ 11$

$= 9\ mod\ 11 = 9$

- Two versions

1. If p is a prime and a is an integer such that p does not divide a, then $a^{p-1} \equiv 1\ mod\ p$
2. If p is a prime and a is an integer, then $a^p \equiv a\ mod\ p$

- Applications:
  1. Helpful for quickly finding a solution to some exponentiations.
  2. Helpful for quickly finding multiplicative inverses if the modulus is a prime.

Fermat's Little Theorem (Contd...)

$Ex: Find\ the\ result\ of\ 8^{-1}\ mod\ 17.$

$$Sol:\ 8^{-1}\ mod\ 17 = 8^{17-2}\ mod\ 17$$
$$= 8^{15}\ mod\ 17$$
$$= 15\ mod\ 17$$

- Application: Helpful for quickly finding multiplicative inverses if the modulus is a prime.
- If p is a prime and a is an integer such that p does not divide a, then $a^{-1}\ mod\ p = a^{p-2}\ mod\ p$

Euler's Theorem

$$a^{\emptyset(n)} \equiv 1 \, mod \, n$$

$$a^{k\times\emptyset(n)+1} \equiv a \, mod \, n$$

- Basically, this is a generalization of Fermat's Little theorem.
- Two Versions
  1. If a and n are coprimes, then $a^{\emptyset(n)} \equiv 1 \, mod \, n$
  2. If $n = p \times q$, $\mathrm{a} < \mathrm{n}$, and k an integer, then $a^{k\times\emptyset(n)+1} \equiv a \, mod \, n$

Generating Primes

$$M_2 = 2^2 - 1 = 3$$
$$M_3 = 2^3 - 1 = 7$$
$$M_5 = 2^5 - 1 = 31$$
$$M_7 = 2^7 - 1 = 127$$
$$M_{11} = 2^{11} - 1 = 2047$$

- Mersenne Primes: Mersenne defined a formula, called Mersenne numbers.

$$M_p = 2^p - 1$$

- Failed at M_{11} = 2047 = 23 x 89

Generating Primes (Contd…)

$$F_1 = 2^{2(1)} - 1 = 3$$
$$F_2 = 17$$
$$F_3 = 257$$
$$F_4 = 65537$$
$$F_5 = 4294967297$$

- Fermat Primes: Fermat found a formula to generate primes as

$$F_n = 2^{2n} - 1$$

- Tested upto F_4, but failed at F_5, where

$$F_5 = 4294967297 = 641 \times 6700417$$

By the end of this session…

- Discuss some primality test algorithms and their efficiencies.

Primality Testing

- Asymmetric Cryptography needs large primes.
- Generating primes have failed to produce large primes.
- Choose a large random number and test it to be sure that it is a prime.
- Algorithms that deal with primality testing can be divided into two categories:
  - Deterministic algorithms
  - Probabilistic algorithms
- Deterministic algorithms always gives the correct answer, but less efficient.
- Probabilistic algorithms gives an answer that is correct most of the time, but not all of the time.

Deterministic algorithms - Divisibility Algorithm

- Most elementary deterministic test for primality.
- Choose a number n, divide with all numbers smaller than $\sqrt{n}$, if any of these numbers divide n, then n is not a prime number.
- Algorithm can be improved by testing only odd numbers.
- If n_b is the number of bits in n, the complexity for this algorithm is $O(2^{n_b})$.
- Algorithm seem very inefficient for large integers.

Deterministic algorithms - AKS Algorithm

- Proposed by Agrawal, Kayal and Saxena in the year 2002.
- The algorithm uses the fact that

$$(x-a)^p \equiv (x^p - a) \bmod p$$

- The algorithm reduced the complexity to $O\left(\left(log_2^{n_b}\right)^{12}\right)$.

Probabilistic Algorithms - Fermat Test

$Ex: Prove\ number\ 561\ is\ a\ prime$

$Sol:\ 2^{561\ -1} \equiv 1\ mod\ 561$

$2^{560}\ mod\ 561 = 1$

$So, 561\ is\ a\ prime\ number\ according\ to\ Fermat\ test$

$but, 561\ is\ a\ not\ prime\ number,\ because\ 561 = 33\ \times 17$

- Uses the fact in Fermat little theorem
- If n is a prime, then

$$a^{n-1} \equiv 1\ mod\ n$$

- If n does not satisfies the condition then it is a composite number.
- Some composite numbers may pass the Fermat test.

Probabilistic Algorithms – Miller – Rabin Test

$Ex: Is\ 53\ prime?$

$Step\ -1: 52 = 2^k.m$

$52 = 2^1.26$

$52 = 2^2.13 \quad k = 2, m = 13$

$\cancel{52 = 2^3.6.5}$

$Step\ -2: a = 2, 1 < a < n - 1$

$Step\ -3:\ b_0 = 2^{13}\ mod\ 53 = 30\ mod\ 53$

$Step\ -4:\ b_1 = 30^2\ mod\ 53 = 52\ mod\ 53$

$-1\ mod\ 53$

$So, 53\ is\ probably\ prime.$

- Specifies whether n is a prime or composite based on Square roots of 1. i.e., +1 or -1.
- Steps:
    1. Find $n - 1 = 2^k.m$
    2. Choose a such that 1<a<n-1
    3. Compute $b_0 = a^m\ mod\ n$
    4. Continue step 3 as a = b_0, and m =2 until $b_i = +1\ or\ -1$, If the result is -1 then the number is probably prime, or it is a composite number.

Ex: Is 4033 a prime?

$Step\ -1: 4032 = 2^k.m$

$4032 = 2^1.2016$

$4032 = 2^2.1008$

$4032 = 2^3.504$

$4032 = 2^4.252$

$4032 = 2^5.126$

$4032 = 2^6.63 \quad k = 6, m = 63$

$\cancel{4032 = 2^7.31.5}$

$Step\ -2: a = 2\ , 1 < a < n - 1$

$Step\ -3:\ b_0 = 2^{63}\ mod\ 4033 = 3521\ mod\ 4033$

$Step\ -4:\ b_1 = 3521^2\ mod\ 4033 = 4032\ mod\ 4033$

$-1\ mod\ 4033$

$So, 4033\ is\ probabily\ prime.$

$but, 4033\ is\ not\ a\ prime, because\ 37 \times 109.$

$Exercise: Take\ a = 3\ and\ check\ whether\ 4033\ is\ prime\ or\ not?$

By the end of this session…

- Explain various factorization methods.
- Explain the Chinese Remainder Theorem with examples.

Factorization

$$n = p_1^{e1} \times p_2^{e2} \times \cdots \times p_k^{ek}$$

$$20 = 2^2 \times 5^1$$

$$100 = 2^2 \times 5^2$$

$$GCD(a, b): a = p_1^{x1} \times p_2^{x2} \times \cdots \times p_k^{xk}$$

$$b = p_1^{y1} \times p_2^{y2} \times \cdots \times p_k^{yk}$$

$$GCD(a, b) = p_1^{\min(x1,y1)} \times p_2^{\min(x2,y2)} \times \cdots \times p_k^{\min(xk,yk)}$$

$$LCM(a, b) = p_1^{\max(x1,y1)} \times p_2^{\max(x2,y2)} \times \cdots \times p_k^{\max(xk,yk)}$$

$$a \times b = GCD(a, b) \times LCM(a, b)$$

- Plays an important role in security of several public key cryptographic algorithms such as RSA.
- Fundamental Theorem of Arithmetic: Any positive greater than one can be written uniquely in the prime factorization form.
- Immediate applications of Factorization
  - GCD
  - LCM

Factorization Methods – Trial Division Method

- Simplest and least efficient algorithm.
- Try dividing all positive integers starting from 2 to $\sqrt{n}$.
- Normally efficient if $n<2^{10}$, but inefficient and infeasible for factoring large integers.
- The complexity is exponential.

Factorization Methods – Fermat Method

```
Fermat_Factorization(n)
{
    x = √n
    while(x < n)
    {
        w = x^2 – n
        if (w is perfect square) { y = √n,  a=x+y, b= x – y, return a and b}
        x = x+1
    }
}
```

- Divides a number into two positive integers a and b (not necessarily a prime), so that $n = a \times b$
- The Fermat method is based on the fact that

$$n = x^2 - y^2$$

Where

$$a = (x + y)\ and\ b = (x - y)$$

- The complexity is subexponential

Chinese Remainder Theorem

$$x = a_1 \, mod \, m_1$$
$$x = a_2 \, mod \, m_2$$
$$\dots$$
$$x = a_k \, mod \, m_k$$

- Is meant for solving set of congruent equations with one variable but different moduli.
- The set of equations have a unique solution if the moduli are relatively prime. i.e., GCD(m_1, m_2, …, m_k) = 1

Chinese Remainder Theorem - Working

$$x = 2\ mod\ 3$$

$$x = 3\ mod\ 5$$

$$x = 2\ mod\ 7$$

$$M = 3 \times 5 \times 7 = 105$$

$$M_1 = \frac{105}{3} = 35, M_2 = \frac{105}{5} = 21, M_3 = \frac{105}{7} = 15$$

$$The\ inverses\ are\ M_1^{-1} = 2, M_2^{-1} = 1, M_3^{-1} = 1$$

$$x = (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) mod\ 105$$

$$23\ mod\ 105$$

$$23 \equiv 2\ mod\ 3, 23 \equiv 3\ mod\ 5, 23\ \equiv 2\ mod\ 7$$

1. Find $M = m_1 \times m_2 \times \cdots m_k$
2. Find $M_1 = M/m_1, M_2 = M/m_2, \ldots, M_k = M/m_k$.
3. Find Multiplicative inverse of M_1, M_2, …, Mk using moduli (m_1, m_2, …, m_k) as $M_1^{-1}, M_2^{-1}, \ldots, M_k^{-1}$.
4. Solution

$$x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1}$$

Exercise: Solve the following set of congruent equations

$x = 3\ mod\ 7$

$x = 3\ mod\ 13$

$x = 0\ mod\ 12$

$$M = 7 \times 13 \times 12 = 1092$$

$$M_1 = \frac{1092}{7} = 156, M_2 = \frac{1092}{13} = 84, M_3 = \frac{1092}{12} = 91$$

$$The\ inverses\ are\ M_1^{-1} = 4, M_2^{-1} = 11, M_3^{-1} = 7$$

$$x = (3 \times 156 \times 4 + 3 \times 84 \times 11 + 0 \times 91 \times 7)\ mod\ 1092$$

$$276\ mod\ 1092$$

$$276 \equiv 3\ mod\ 7, 276 \equiv 3\ mod\ 13, 276\ \equiv 0\ mod\ 12$$

By the end of this session…

- Explain the concept of Quadratic congruence

Quadratic Congruence

$$x^2 \equiv a \bmod n$$

- Solving the equation of type
$$a_2x^2 + a_1x + a_0 \equiv 0 \bmod n$$
- Asymmetric Cryptographic algorithms are more dependent on equations
$$x^2 \equiv a \bmod n$$

Where $a_2 = 1$, $a_1=0$ and $a_0=0$.

- Such equations are called Quadratic congruence.

Quadratic Congruence Modulo a Prime

$Eg\colon\ x^2 \equiv 3\ mod\ 11$

$Has\ two\ solutions$

$x = 5\ mod\ 11\ and\ x = -5\ mod\ 11$

$5^2\ mod\ 11 = 3\ and\ (-5)^2\ mod\ 11$

$Eg\colon\ x^2 \equiv 2\ mod\ 11$

$Has\ no\ Solution$

- Finding the solution for an equation of form

$$x^2 \equiv a\ mod\ p$$

Where p is a prime, a is an integer.

- This type of equation has either no solution or exactly two solutions.

Quadratic Residues and Nonresidues

$Eg: Z_{11}^{*} = \{1,2,3,4,5,6,7,8,9,10\}$

$1^2 \; mod \; 11 = 1 \qquad 6^2 \; mod \; 11 = 3$

$2^2 \; mod \; 11 = 4 \qquad 7^2 \; mod \; 11 = 5$

$3^2 \; mod \; 11 = 9 \qquad 8^2 \; mod \; 11 = 9$

$4^2 \; mod \; 11 = 5 \qquad 9^2 \; mod \; 11 = 4$

$5^2 \; mod \; 11 = 3 \qquad 10^2 \; mod \; 11 = 1$

$QR_{11} = \{1, 3, 4, 5, 9\}$

$QNR_{11} = \{2, 6,7, 8, 10\}$

- In the equation $x^2 \equiv a \; mod \; p$, a is called quadratic residue (QR), if the equation has two solutions.
- 'a' is said to be quadratic nonresidue (QNR), if the equation has no solutions.
- In Z_p^* with p-1 elements, exactly

$$(p-1)/2$$

elements are quadratic residues.

Back...

Exponentiation and Logarithm

$$Exponentiation: y = a^x$$

$$Logarithm: x = log_a\, y$$

$$Exponentiation: y = a^x \; mod\; p$$

$$Logarithm: x = log_{a,p}\, y$$

- Most of the Asymmetric Cryptographic algorithms are based on two operations
  - Exponentiation
  - Logarithm
- These two operations are inverses of each other.

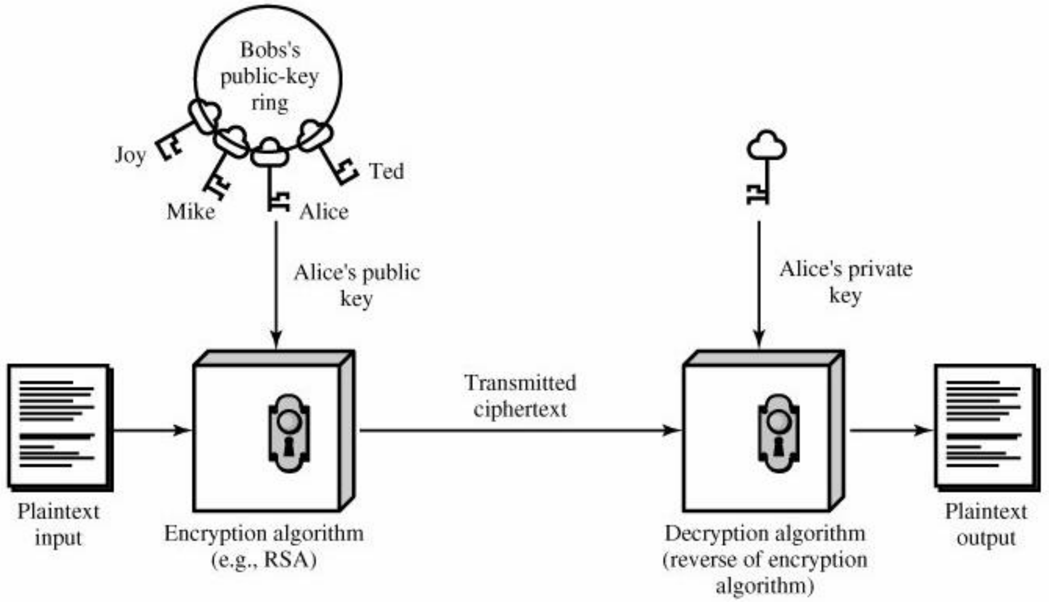
Discrete Logarithm

- Finite multiplicative group: $G = \langle Z_n^*, x \rangle$
- Order of the group: Number of elements in Z_n^*
- Order of an Element: Number of elements in cyclic subgroup generated by the element.
- Primitive Roots: Meant for multiplicative group, where the order of the group is equal to order of the element, then that element is a primitive root of the group

By the end of this session…

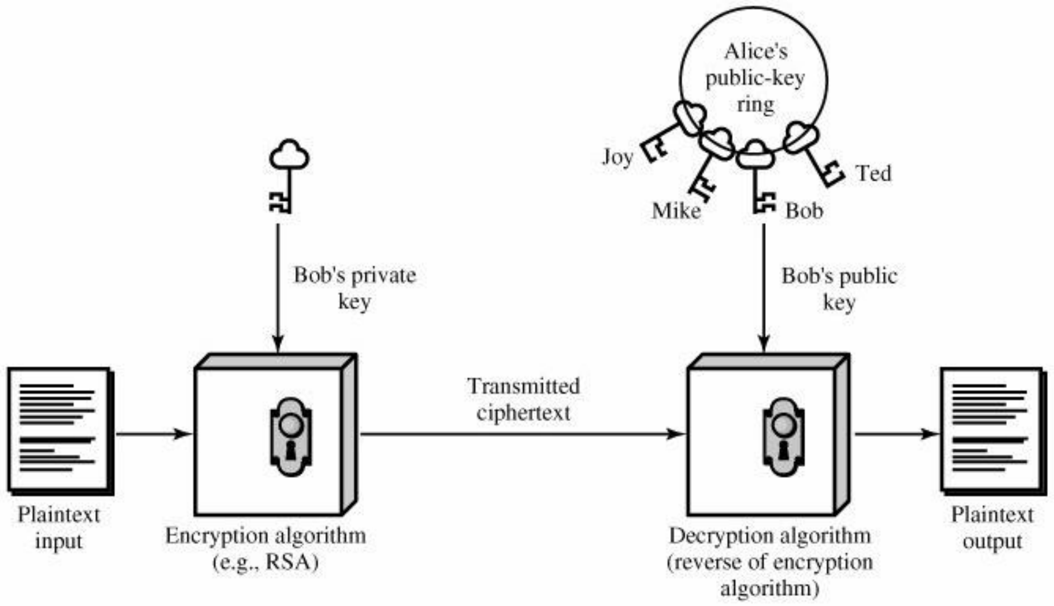
- Describe the concept of asymmetric key cryptosystems
- Discuss the concept of RSA cryptosystem.

Asymmetric Cryptography



- Every user generates two keys to participate in Asymmetric Cryptography.
  - Public Key (PU_K)
  - Private Key (PR_K)
- Users share their public key with all the participants in the network, but, keeps private key secret with them.

Asymmetric Cryptography (Contd...)



- Two usecases
  - Confidentiality (Encipherment)
  - Authentication (Signature)
- Encryption is done with the public key of the receiver and decryption is done with the private key of the receiver.
- Signature is done with sender's private key and verified through sender's public key at receiver's side

RSA Cryptosystem

$$C = M^e \bmod n$$

$$M = C^d \bmod n = (M^{ed}) \bmod n$$

- Named after inventors Rivest, Shamir, Adleman (RSA).
- First published in 1978.
- Is a block cipher in which plaintext and cipher text are integers between 0 and n-1.
- Typical size of n is 1024 bits, i.e., 309 decimal digits.

RSA Key Generation

1. $P = 5 \; and \; q = 11$
2. $n = 5 \times 11 = 55$
3. $\emptyset(n) = 4 \times 10 = 40$
4. $e = 7 \; as \; \gcd(40, 7) = 1$
5. $d = 43 \; as \; 43 = 7^{-1} \; mod \; 40$
6. $Public \; key \; (7,55),$
$Private \; key \; (43, 40)$

1. Both sender and receiver generates their pair of keys (Public, Private).
   i. Selects two large primes p and q.
   ii. Computes $\mathrm{n} = \mathrm{p} \times q$
   iii. Calculates $\emptyset(n) = (p-1) \times (q-1)$
   iv. Selects integer e, such that $\gcd(\emptyset(n), e) = 1$
   v. Calculate d, such that $d = e^{-1} \; mod \; \emptyset(n)$
   vi. Public key (e, n) and Private key (d,$\emptyset(n)$)
2. Users share their public keys

RSA Encryption & Decryption

$$C = 3^7 \bmod 55$$
$$= 42 \bmod 55$$

Sender

$$M = 42^{43} \bmod 55$$
$$= 3 \bmod 55$$

Receiver

- Compute

$$C = M^e \bmod n$$

Where e is the public key of the receiver.

- Compute

$$M = C^d \bmod n$$

Where d is the private key of the receiver

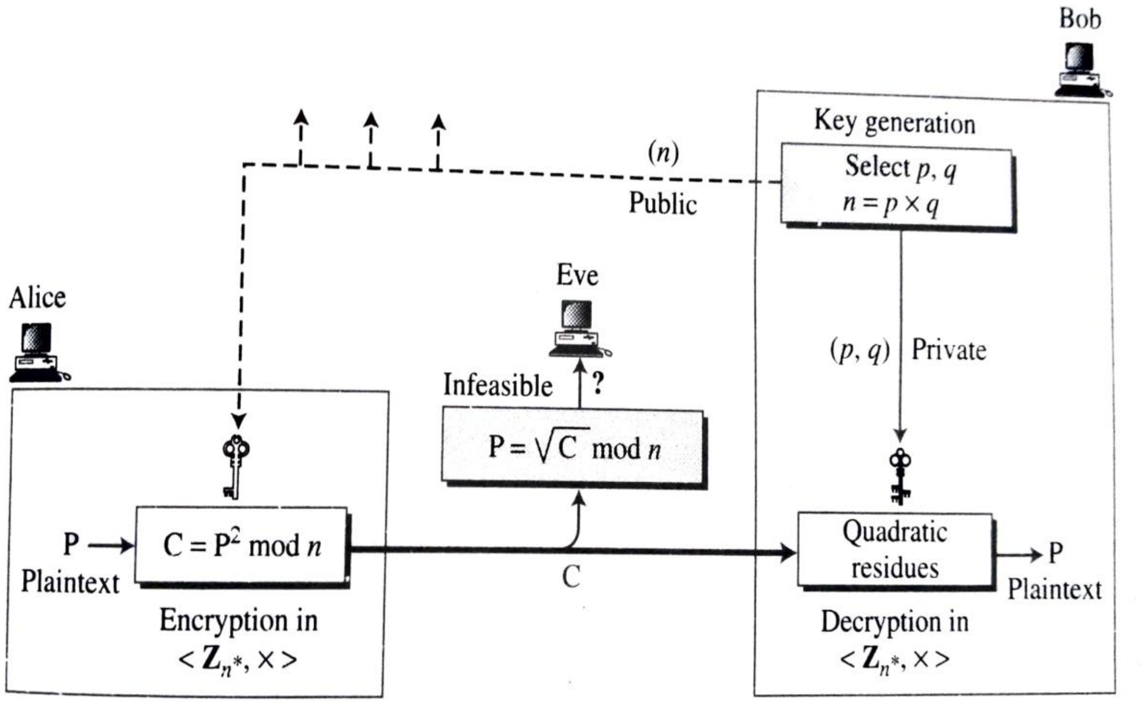
Attacks on RSA

- Factorization
- Chosen-Ciphertext
- Plaintext

By the end of this session…

- Explain Rabin cryptosystem and describe the procedure of key generation, encryption and decryption.

Rabin Cryptosystem



- Devised by M. Rabin
- Is a variation of the RSA cryptosystem, where RSA is based on exponentiation congruence and Rabin is based on quadratic congruence.
- Encryption: $C = M^2 \ mod \ n$
- Decryption: $M = C^{1/2} \ mod \ n$

Rabin Key Generation

Key Generation

1. Users selects two large primes p and q, prime must be in the form $p \equiv 3 \; mod \; 4$
2. Calculates n = p x q
3. Public key = n and private key (p,q)

Example

1. p = 23 and q = 7
2. Calculates n = 23 x 7 = 161
3. Public key = 161 and private key (23,7)

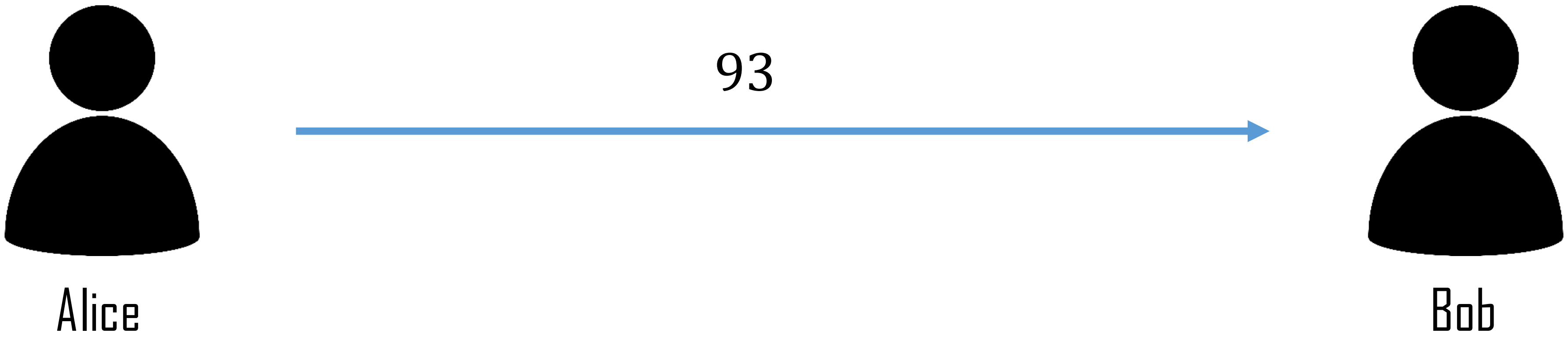
Encryption

Bob

1. $p = 23$ and $q = 7$
2. Calculates $n = 23 \times 7 = 161$
3. Public key = 161 and private key (23,7)

$$C = M^2 \, mod \, n$$

$$93 = 24^2 \, mod \, 161$$

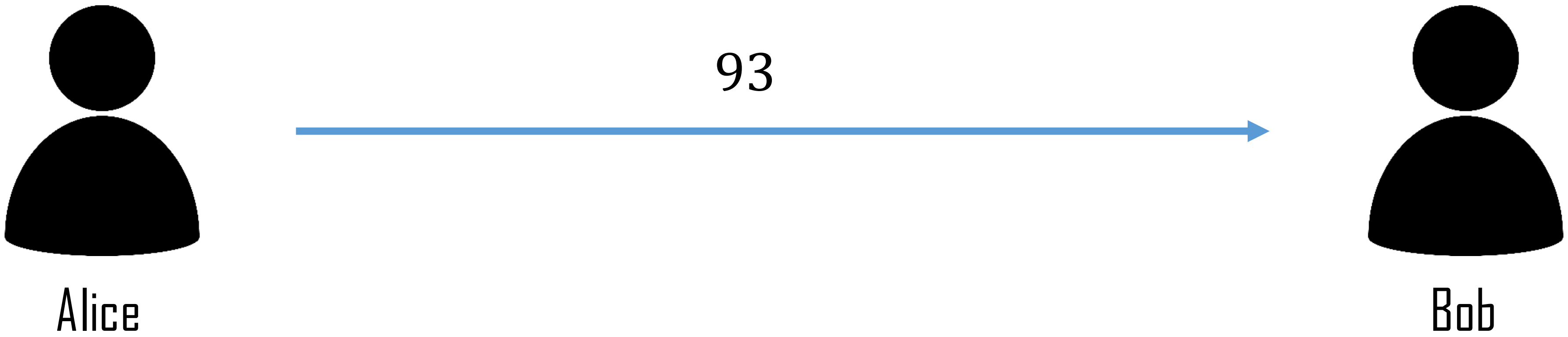


Decryption

$$a_{1,2} = \pm\left(C^{(p+1)/4}\right) \, mod \, p$$

$$b_{1,2} = \pm\left(C^{(q+1)/4}\right) \, mod \, q$$

$$(a_1, b_1), (a_1, b_2), (a_2, b_1), (a_2, b_2)$$



Decryption

$$a_{1,2} = \pm\left(C^{(p+1)/4}\right) mod\ p$$

$$b_{1,2} = \pm\left(C^{(q+1)/4}\right) mod\ q$$

$$(a_1, b_1), (a_1, b_2), (a_2, b_1), (a_2, b_2)$$

Use Chinese Remainder Theorem to solve these congruences

$$a_1 = \left(93^{(23+1)/4}\right) mod\ 23 = 1\ mod\ 23$$

$$a_2 = -\left(93^{(23+1)/4}\right) mod\ 23 = 22\ mod\ 23$$

$$b_1 = \left(93^{(7+1)/4}\right) mod\ 7 = 4\ mod\ 7$$

$$b_2 = -\left(93^{(7+1)/4}\right) mod\ 7 = 3\ mod\ 7$$

$$x1 = (1\ mod\ 23, 4\ mod\ 7)$$

$$x2 = (1\ mod\ 23, 3\ mod\ 7)$$

$$x3 = (22\ mod\ 23, 4\ mod\ 7)$$

$$x4 = (22\ mod\ 23, 3\ mod\ 7)$$

Decryption

$x \equiv 1 \; mod \; 23$

$x \equiv 4 \; mod \; 7$

$x = 116$

$x \equiv 1 \; mod \; 23$

$x \equiv 3 \; mod \; 7$

$x = 24$

$x \equiv 22 \; mod \; 23$

$x \equiv 4 \; mod \; 7$

$x = 137$

$x \equiv 22 \; mod \; 23$

$x \equiv 3 \; mod \; 7$

$x = 45$

By the end of this session…

- Describe the working of Elgamal cryptosystem

Elgamal Cryptosystem

- Elgamal cryptosystem is based on discrete logarithm problem
- If p is a very large prime, e_1 is a primitive root in the group $G = < Z_p^*, \times >$ and r is an integer, then

$$e_2 = e_1^r \ mod\ p$$

is easy to compute. But given e_2, e_1, p, it is infeasible to calculate

$$r = log_{e_1, e_2}\ mod\ p$$

Key Generation

Key Generation

1. Select a prime p,
2. Select e_1, primitive root of p.
3. Select d, as a random integer, such that $1 \leq d \leq p - 2$
4. Compute $e_2 = e_1^d \; mod \; p$
5. Public key = (e_1, e_2, p), Private key = d

Example

1. p = 11
2. e_1 = 2
3. d = 3
4. $e_2 = 2^3 \; mod \; 11 = 8 \; mod \; 11$
5. Public key = (2, 8, 11) and Private key = 3

Derivation of Encryption and Decryption process

Sender

1. Selects a random integer r in $G =< Z_p^*, \times>$
2. Computes $C_1 = e_1^r \; mod \; p$
3. Computes $C_2 = e_2^r \times M \; mod \; p$

Receiver

1. $C_1 \; and \; C_2$
2. $M = [C_2 \times (C_1^d)^{-1}] \; mod \; p$

$$[C_2 \times (C_1^d)^{-1}] \; mod \; p = \left[(e_2^r \times M) \times \left(e_1^{rd}\right)^{-1}\right] mod \; p = \left(e_1^{dr}\right) \times M \times \left(e_1^{rd}\right)^{-1} mod \; p = M \; mod \; p$$

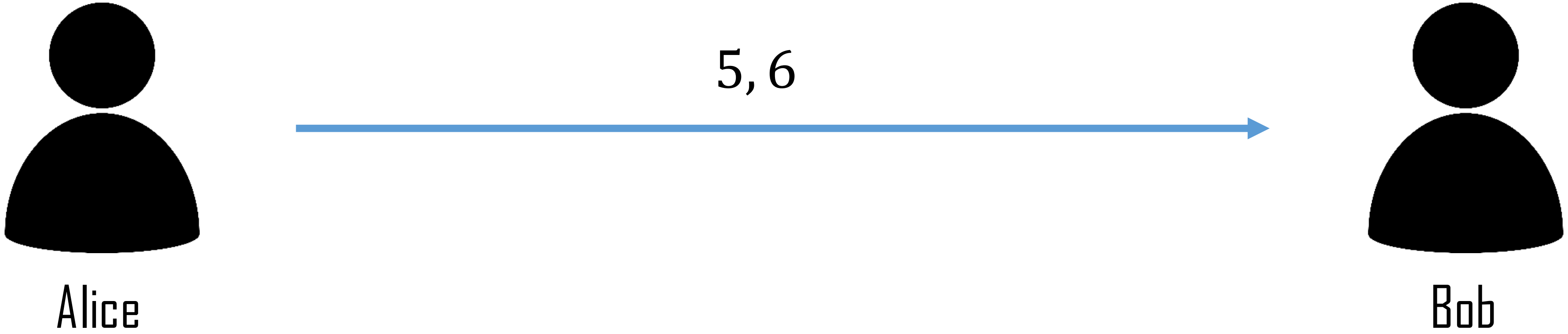
Encryption

Encryption

1. Selects a random integer r in $G = < Z_p^*, \times >$, r = 4
2. Computes $C_1 = e_1^r \bmod p = 2^4 \bmod 11 = 5 \bmod 11$
3. Computes $C_2 = e_2^r \times M \bmod p = 8^4 \times 7 \bmod 11 = 6 \bmod 11$

Bob

1. p = 11
2. e_1 = 2
3. d = 3
4. $e_2 = 2^3 \bmod 11 = 8 \bmod 11$
5. Public key = (2, 8, 11) and Private key = 3

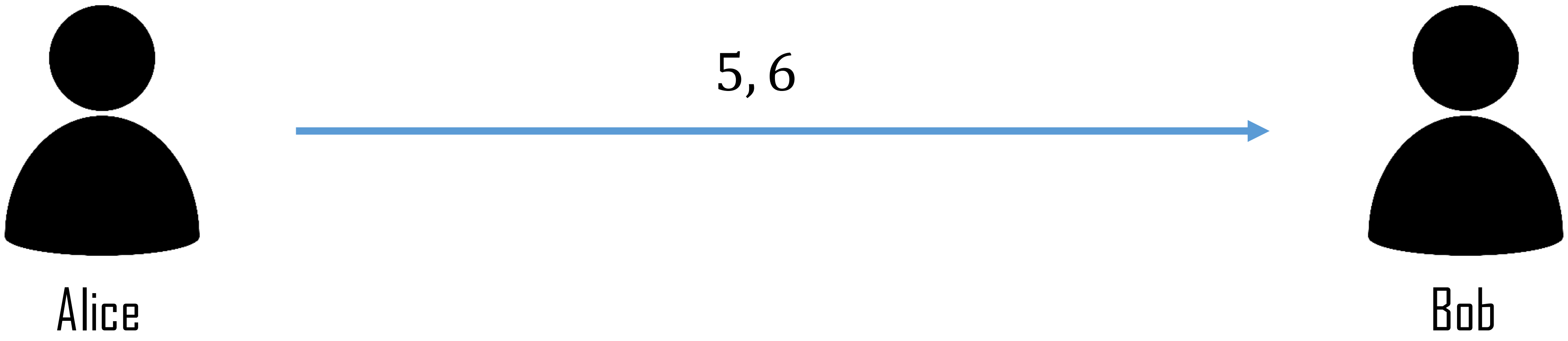


Decryption

Decryption

1. $C_1 = 5 \; and \; C_2 = 6$
2. $M = [C_2 \times (C_1^d)^{-1}] \; mod \; p$

$$M = [6 \times (5^3)^{-1}] \; mod \; 11 = 7 \; mod \; 11$$



Security of Elgamal

- Low Modulus attack
- Known plaintext attack

By the end of this session…

- Explain the concept of Elliptic curve cryptosystems

Elliptic Curve Cryptography

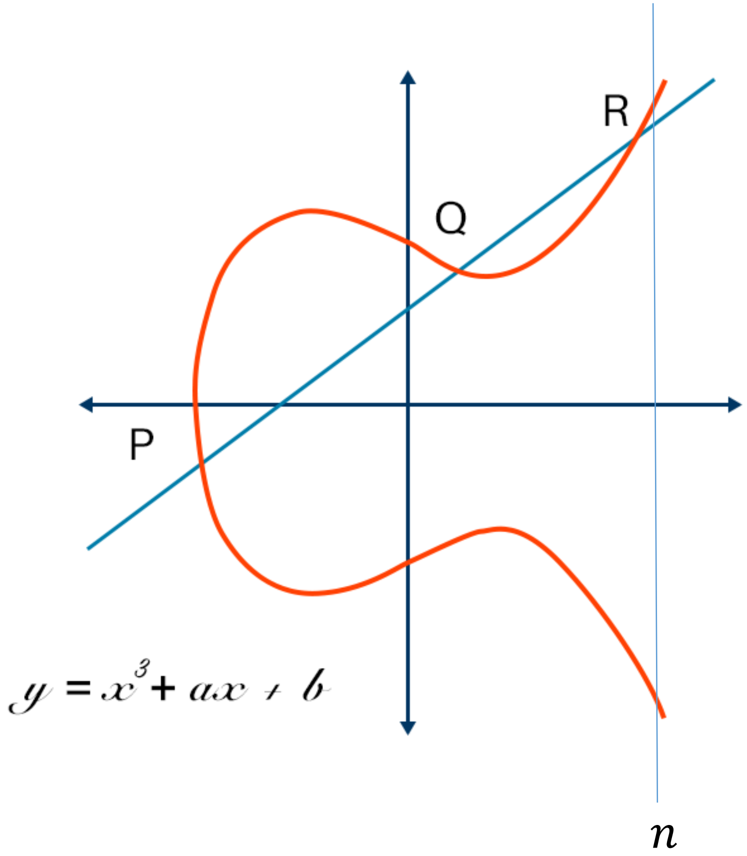
- Provides equal security with smaller key size

RSA	ECC
3072	256
7680	384

- Reduced the processing overhead
- Trapdoor function

$$A \rightarrow B$$
$$B \nrightarrow A$$

Elliptic curve cryptography



- Elliptic curves defined by the cubical functions of form

$$y^2 = x^3 + ax + b$$

are used for Elliptic curve cryptography.

- Symmetric to the x-axis
- Draw a line on the curve, touches maximum of 3 points.
- Curve goes infinite over x and y axis but we are limiting it with the value of n.
- Points on the curve are called Affine Points
- Trapdoor function: $Q = kP$, but with the knowledge of P, Q we can't find the value of k.

Elliptic Curve Cryptography

Global Public Elements

1. $E_q(a, b)$: Elliptic curve with parameters a,b and q (Prime no. or an integer of form 2^m
2. G: Generator point on the curve whose order equal to the order of the group G=<{Points on curve}, +>

User A key generation

1. Select a private key $n_a, n_a < n$
2. Calculate public key p_a

$$p_a = n_a \times G$$

User B key generation

1. Select a private key $n_b, n_b < n$
2. Calculate public key p_b

$$p_b = n_b \times G$$

Calculation of Secret Key

1. User A: $K = n_a \times p_b$
2. User B: $K = n_b \times p_a$

Encryption & Decryption

Encryption

1. Let the message be M.
2. Convert the message M into a point on the elliptic curve and it be p_m
3. The Cipher point will be

$$C_m = \{kG, p_m + kp_b\}$$

Decrytion

1. Multiply 1st coordinate in the received point with private key of receiver

$$kG \times n_b$$

2. Then Subtract it from 2nd coordinate

$$p_m + kp_b - (kG \times n_b)$$

Justification

1. $p_m + kp_b - (kG \times n_b)$, we know $p_b = G \times n_b$
2. $p_m + kp_b - kp_b = p_m$

Exercises

1. Find all QRs and QNRs in $Z_{13}^*, Z_{17}^*, Z_{23}^*$.
2. Solve the following congruence:
   i. $x^2 \equiv 4 \; mod \; 7$
   ii. $x^2 \equiv 5 \; mod \; 11$
3. For the group $G = < Z_{11}^*, \times >$:
   i. Find the order of the group
   ii. Find the order of each element in the group
   iii. Find the primitive roots in the group
4. In RSA:
   i. Given p=19, q=23, and e=3 find d.
   ii. Given n=221 and e=5, find d.


Thank you!