R.M.K GROUP OF ENGINEERING INSTITUTIONS

R.M.K
GROUP OF INSTITUTIONS

R.M.K
GROUP OF
INSTITUTIONS

Please read this disclaimer before proceeding:

22CS701- CRYPTOGRAPHY AND CYBER SECURITY (Lab Integrated)

Unit-III

Department: Computer Science and Engineering

Batch/Year : 2022-2026/IV

Created by:

Dr. A.Thilagavathy/ Associate Professor/CSE/RMKEC

Dr.D.Naveen Raju /Associate Professor/CSE/RMKEC

Ms.K.Padmapriya/ Associate Professor/CSE/RMDEC

Dr. J. Sherine Glory/Assistant Professor/CSE/RMDEC

Dr.Anish T P/Associate Professor/CSE/RMKCET

Mr.Vinoth Kumar V/ Assistant Professor/CSE(CS)/RMKCET

Date: 17.08.2025

R.M.K GROUP OF INSTITUTIONS

Table of Contents

22CS701-CRYPTOGRAPHY AND CYBER SECURITY
(Lab Integrated)

COURSE OBJECTIVES

The Course will enable learners to:

- Understand the fundamentals of network security and security architecture.
- Learn the different symmetric key cryptographic algorithms.
- Study the various asymmetric key cryptographic algorithms and techniques.
- Know the importance of message authentication and integrity.
- Learn the various cyber-crimes and cyber security

PREREQUISITE

- 22MA201 Transforms and Numerical Methods
- 22CS501 Computer Networks

22CS701 CRYPTOGRAPHY AND CYBER SECURITY (Lab Integrated)

SYLLABUS

22CS701 CRYPTOGRAPHY AND CYBER SECURITY 3 0 2 4

UNIT I INTRODUCTION TO SECURITY 9+6

Computer Security Concepts – The OSI Security Architecture – Security Attacks – Security Services and Mechanisms – A Model for Network Security – Classical encryption techniques: Substitution techniques, Transposition techniques, Steganography –Foundations of modern cryptography: Perfect security – Information Theory – Product Cryptosystem – Cryptanalysis.

List of Exercise/Experiments:

1. Perform encryption, decryption using the following substitution techniques (i) Ceaser cipher, (ii) playfair cipher iii) Hill Cipher iv) Vigenere cipher
2. Perform encryption and decryption using following transposition techniques i) Rail fence ii) row & Column Transformation

UNIT II SYMMETRIC CIPHERS 9+6

Number theory – Algebraic Structures – Modular Arithmetic - Euclid's algorithm – Congruence and matrices – Group, Rings, Fields, Finite Fields SYMMETRIC KEY CIPHERS: SDES – Block Ciphers – DES, Strength of DES – Differential and linear cryptanalysis – Block cipher design principles – Block cipher mode of operation – Evaluation criteria for AES – Pseudorandom Number Generators – RC4 – Key distribution.

List of Exercise/Experiments:

1. Apply DES algorithm for practical applications.
2. Apply AES algorithm for practical applications.

UNIT III ASYMMETRIC CRYPTOGRAPHY 9+6

MATHEMATICS OF ASYMMETRIC KEY CRYPTOGRAPHY: Primes – Primality Testing –Factorization – Euler's totient function, Fermat's and Euler's Theorem – Chinese Remainder Theorem – Exponentiation and logarithm ASYMMETRIC KEY CIPHERS: RSA cryptosystem – Key distribution – Key management – Diffie Hellman key exchange -– Elliptic curve arithmetic – Elliptic curve cryptography.

List of Exercise/Experiments:

1. Implement RSA Algorithm using HTML and JavaScript.
2. Implement the Diffie-Hellman Key Exchange algorithm for a given problem.
3. Calculate the message digest of a text using the SHA-1 algorithm.

22CS701 CRYPTOGRAPHY AND CYBER SECURITY (Lab Integrated)

SYLLABUS

22CS701 CRYPTOGRAPHY AND CYBER SECURITY 3 0 2 4

UNIT IV INTEGRITY AND AUTHENTICATION ALGORITHMS 9+6

Authentication requirement – Authentication function – MAC – Hash function – Security of hash function: HMAC, CMAC – SHA – Digital signature and authentication protocols – DSS – Schnorr Digital Signature Scheme – ElGamal cryptosystem – Entity Authentication: Biometrics, Passwords, Challenge Response protocols – Authentication applications – Kerberos MUTUAL TRUST: Key management and distribution – Symmetric key distribution using symmetric and asymmetric encryption – Distribution of public keys – X.509 Certificates

List of Exercise/Experiments:

1. Implement the SIGNATURE SCHEME - Digital Signature Standard.
2. Demonstrate intrusion detection system (ids) using any tool eg. Snort or any other s/w

UNIT V CYBER CRIMES AND CYBER SECURITY 9+6

Cyber Crime and Information Security – classifications of Cyber Crimes – Tools and Methods – Password Cracking, Keyloggers, Spywares, SQL Injection – Network Access Control – Cloud Security – Web Security – Wireless Security

List of Exercise/Experiments:

1. Automated Attack and Penetration Tools

a.Exploring N-Stalker, a Vulnerability Assessment Tool

2. Defeating Malware

i) Building Trojans ii) Rootkit Hunter

COURSE OUTCOMES

CO1	Understand cryptographical concepts.
CO2	Implement various cryptographic algorithms
CO3	Evaluate and apply network security protocols, to secure communications over networks
CO4	Identify common security threats and vulnerabilities and assess their impact on network security
CO5	Implement access control mechanisms and authentication techniques to protect information systems.
CO6	Develop and propose security policies and best practices for securing networks and information systems

CO-PO MAPPING

COs	PO's/PSO's														
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO1	3	3	3	2	2	-	-	2	2	1	-	2	2	2	1
CO2	3	3	3	2	2	-	-	2	2	1	-	2	2	2	1
CO3	3	3	3	2	2	-	-	2	2	1	-	2	2	2	1
CO4	3	3	3	2	2	-	-	2	2	1	-	2	2	2	1
CO5	3	3	3	2	2	-	-	2	2	1	-	2	2	2	1
CO6	3	3	3	2	2	-	-	2	2	1	-	2	2	2	1

1 – Low, 2 – Medium, 3 – Strong

LECTURE PLAN

S No	Topics	No of periods	Proposed date	Actual Lecture Date	Pertaining CO	Taxonomy level	Mode of delivery
1	Primes , Primality Testing , Factorization	1	29-08-2025		CO3	K1	ICT Tools
2	Euler's totient function, Fermat's and Euler's Theorem	1	29-08-2025		CO3	K3	ICT Tools
3	Chinese Remainder Theorem –	1	01-09-2025		CO3	K3	ICT Tools
4	Exponentiation and logarithm	1	02-09-2025		CO3	K3	ICT Tools
5	RSA cryptosystem	1	03-09-2025		CO3	K3	ICT Tools
6	Key distribution, Key management	1	04-09-2025		CO3	K2	ICT Tools
7	Diffie Hellman key exchange	1	04-09-2025		CO3	K3	ICT Tools
8	Elliptic curve arithmetic	1	05-09-2025		CO3	K3	ICT Tools
9	Elliptic curve cryptography.	1	05-09-2025		CO3	K3	ICT Tools
10	Implement RSA Algorithm using HTML and JavaScript.	1	06-09-2025		CO3	K3	ICT Tools
11	Implement RSA Algorithm using HTML and JavaScript.	1	06-09-2025		CO3	K3	ICT Tools
12	Implement the Diffie-Hellman Key Exchange algorithm for a given problem	1	08-09-2025		CO3	K3	ICT Tools
13	Implement the Diffie-Hellman Key Exchange algorithm for a given problem	1	09-09-2025		CO3	K3	ICT Tools
14	Calculate the message digest of a text using the SHA-1 algorithm.	1	10-09-2025		CO3	K3	ICT Tools
15	Calculate the message digest of a text using the SHA-1 algorithm.	1	11-09-2025		CO3	K3	ICT Tools

ACTIVITY BASED LEARNING

S NO	TOPICS	Link
1	Key distribution	https://www.youtube.com/watch?v=6bUNDR5Zhiw
2	RSA cryptosystem	https://www.youtube.com/watch?v=wXB-V_Keiu8
3	Diffie Hellman key exchange	https://www.youtube.com/watch?v=EAq6_JqRnzs https://www.youtube.com/watch?v=cM4mNVUBtHk
3	Elliptic Curve Cryptography	https://www.youtube.com/watch?v=dCvB-mhkT0w

MATHEMATICS OF ASYMMETRIC KEY CRYPTOGRAPHY

Prime

An integer p is said to be a prime if p>=2 and its only divisors are the trivial divisors 1 and p.

An integer greater than 2 that is not prime is said to be composite.

Examples of Prime: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, ...

Examples of Composite: 4, 6, 8, 9, 10, 12, 14, 15,...

Fermat's Theorem

If p is prime and a is a positive integer not divisible by p, then

$$\mathbf{a^{p-1} \equiv 1 \pmod{p}}$$

An alternative form of Fermat's theorem is also useful: If is prime and is a positive integer, then $\mathbf{a^p \equiv p \pmod{p}}$

Example:

$8^{19-1} \equiv 1 \bmod 19$

$8^2 \equiv 7 \bmod 19$ $8^4 \equiv 11 \bmod 19$ $8^8 \equiv 7 \bmod 19$ $8^{16} \equiv 11 \bmod 19$

$8^{18} \equiv 77 \equiv 1 \bmod 19$

Proof:

Consider a set of positive integers less than p: S = {1, 2, … p-1}

Another set X = {a mod p, 2a mod p, … (p-1)a mod p} which is multiple of a mod p the set S.

None of the elements of X is equal to zero because p does not divide a. All elements of X are unique.

S ≡ X mod p (Since X is permutation of S)

Multiplying the numbers in both sets (S and X) and taking the result mod yields

$[1 \times 2 \times \dots (p-1)] \bmod p = [a \times 2a \times \dots (p-1)] \bmod p$

$[a \times 2a \times \dots (p-1)] \equiv [1 \times 2 \times \dots (p-1)] \bmod p$

$a^{p-1} (p-1)! \equiv (p-1) ! \bmod p$

$a^{p-1} \equiv 1 \pmod{p}$

MATHEMATICS OF ASYMMETRIC KEY CRYPTOGRAPHY

❁ Euler's Totient Function

It is defined as the number of positive integers less than n and relatively prime to n. It is denoted by φ (n).

Reduced Residue System modulo n

The set of positive integers less than n and relatively prime to n. (or) The set of all residue classes relatively prime to n.

Example:

Reduced Residue Set: {1, 3, 7, 9} φ (10) = 4. So, Euler's totient function gives the cardinality of the reduced residue set.

- ❖ φ (mn) = φ(m) . φ(n) if gcd (m, n) =1
- ❖ φ (p) = p -1 p is prime
- ❖ φ (p^j) = p^j - p^{j-1}
- ❖ Φ (n) = n $\prod_{p|n}(1-\frac{1}{p})$

Examples:

φ(97) = 96

Φ(343) = φ(7^3) = 7^3 - 7^2 = 343 - 49 = 294

φ (343) = 343. ∏ (1-1/7) = 343.6/7 = 294

φ (72) = φ (8) φ(9) = 4.6 = 24

❁ Euler's Theorem

If a and n are relatively prime, then $a^{\varphi(n)} \equiv 1 \pmod n$.

Alternative form of this theorem is $a^{\varphi(n)+1} \equiv a \pmod n$.

Proof:

φ (n) is the number of positive integers less than n and relatively prime to n.

Consider the set of such integers, labeled as

R = {x_1, x_2, ..., $x_{\varphi(n)}$ }

S = {(ax_1 mod n), (ax_2 mod n), ..., ($ax_{\varphi(n)}$ mod n)}

The set S is a permutation of R, by the following line of reasoning:

1. Because *a* is relatively prime to *n* and x_i is relatively prime to n, ax_i must also be relatively prime to n. Thus, all the members of S are integers that are less than n and that are relatively prime to n.
2. There are no duplicates in S. If $ax_i \bmod n = ax_j \bmod n$, then $x_i = x_j$.

Therefore,

$$\prod_{i=1}^{\varphi(n)} (ax_i \bmod n) = \prod_{i=1}^{\varphi(n)} x_i$$

$$\prod_{i=1}^{\varphi(n)} ax_i \equiv \prod_{i=1}^{\varphi(n)} x_i \bmod n$$

$$a^{\varphi(n)} \times \left[\prod_{i=1}^{\varphi(n)} x_i\right] \equiv \prod_{i=1}^{\varphi(n)} x_i \bmod n$$

$$a^{\varphi(n)} \equiv 1 \pmod n$$

Example:

$6^{\varphi(11)} \equiv 1 \pmod{11}$ $\varphi(11) = 10$

$6^2 \equiv 3 \pmod{11}$

$6^4 \equiv 9 \pmod{11}$

$6^8 \equiv 4 \pmod{11}$

$6^{10} \equiv 4.3 \equiv 12 \equiv 1 \pmod{11}$

❁ Primality Testing

The following are the some of the popular algorithms used for primality algorithms:

- ❖ Fermat Primality Test
- ❖ Solovay-Strassen Primality Test
- ❖ Miller-Rabin Primality Test

All these algorithms are probabilistic and not deterministic. It means that these algorithms determines whether a number is composite or probably prime.

MATHEMATICS OF ASYMMETRIC KEY CRYPTOGRAPHY

Deterministic Algorithm: AKS Primality Test

This algorithm determines whether a number is prime or not with 100% probability.

But this algorithm is not as efficient as Miller-Rabin algorithm.

- **Miller-Rabin Primality Test**

1. Find integers k, q, with k > 0, q odd, so that ($n - 1 = 2^k q$);
2. Select a random integer a, $1 < a < n-1$;
3. if $a^q \bmod n = 1$ then return ("inconclusive");
4. for j = 0 to k -1 do
5. if $a^{2jq} \bmod n = n - 1$ then return ("inconclusive")
6. return("composite");

Example: n=29

$n-1 = 28 = 2^2 \times 7$ where k=2 and q=7. Let a=2.

Test 1: To check if $a^q \bmod n = 1$

$2^7 = 128 \equiv 12 \not\equiv 1$ (So Test 1 fails)

Test 2: To check for j = 0 to k -1 do if $a^{2jq} \bmod n = n - 1$

j=0, $2^{1\times7} \bmod 29 = 2^7 \bmod 29 = 12 \neq 28$

J=1, $2^{2\times7} \bmod 29 = 2^{14} \equiv 144 \equiv 28 \bmod 29$ (Test 2 passes)

Therefore 29 is probably prime.

Probability of a composite number passing Miller-Rabin Test is $(¼)^t$, where t is number of trials or tests with t different values of a. So for t=10, the probability that a nonprime number will pass all ten tests is less than 10^{-6}.

Strong Pseudoprime

If n is composite and passes the Miller-Rabin test for the base a, then n is called a strong pseudoprime to the base.

Example: Show that 2047 is a strong pseudoprime to the base 2.

Let n = 2047 a=2

$n-1 = 2046 = 1023 \times 2^1$

k=1, q=1023

Test 1: $a^q \bmod n = 1$

$2^{1023} \bmod 2047$

$2^{11} \equiv 2048 \equiv 1 \bmod 2047$

$2^{11} \equiv 2^{110} \equiv 2^{990} \equiv 2^{1001} \equiv 2^{1012} \equiv 2^{1023} \equiv 1 \bmod 2047$

$2047 = 23 \times 89$

Since 2047, which is composite number, passes Miller Rabin Test for a=2 is strong pseudoprime to the base 2.

❁ Chinese Remainder Theorem

The CRT says it is possible to reconstruct integers in a certain range from their residues modulo a set of pairwise relatively prime moduli.

Let $\mathbf{M = \prod_{i=1}^{k} m_i}$

where the mi are pairwise relatively prime; that is, $\gcd(m_i, m_j) = 1$ for $1 \le i, j \le k$, and $i \ne j$.

We can represent any integer a in Z_m by a k-tuple whose elements are in Z_m using the following correspondence:

$$\mathbf{A \leftrightarrow (a_1, a_2, \ldots, a_k)}$$

where $A \varepsilon Z_M$, $a_i \varepsilon Z_m$, and $a_i = A \bmod m_i$ for $1 \le i \le k$. The CRT makes two assertions.

1. The mapping of above Equation is a one-to-one correspondence (called a **bijection**) between Z_M and the Cartesian product $Z_{m1} \times Z_{m2} \times \ldots \times Z_{mk}$. That is, for every integer a such that $0 \le a \le M$, there is unique k-tuple $(a_1, a_2, \ldots a_k)$ with $0 \le a_i \le m_i$ that represents it, and for every such k-tuple $(a_1, a_2, \ldots a_k)$, there is a unique integer a in Z_M.
2. Operations performed on the elements of Z_M can be equivalently performed on the corresponding k-tuples by performing the operation independently in each coordinate position in the appropriate system.

First Assertion:

$a_i = A \bmod m_i$ (each a_i is uniquely calculated)

Let $M_i = M/m_i$ for $1 \le i \le k$

$M = m_1 \times m_2 \times \ldots \times m_{i-1} \times m_{i+1} \times \ldots \times m_k$, so that $M_i=0 \pmod{m_j}$ for all $j \neq i$. Then let $\mathbf{c_i = M_i \times (M_i^{-1} \bmod m_i)}$ **for** $\mathbf{1 \le i \le k}$

By the definition of M_i, it is relatively prime to m_i and therefore has a unique multiplicative inverse mod m_i. So the above equation is well defined and produces a unique value. We can now compute

$A = (\sum_{i=1}^{k} a_i \, ci \,) \pmod{M}$

#Problem: Solve the following simultaneous linear congruences using CRT.

$X \equiv 1 \pmod 5$

$X \equiv 2 \pmod 7$

$X \equiv 3 \pmod 9$

Solution:

$a_1=1, a_2=2, a_3=3$ and $m_1 = 5, m_2 = 7, m_3 =9$

$M = 5 \times 7 \times 9 = 315$

$X = \Sigma \, a_i \, c_i \pmod M$

$c_i = M_i \times (M_i^{-1} \bmod m_i)$

$M_i = M/m_i$

$M_1 = 315/5 = 63$

$M_2 = 315/7 = 45$

$M_3 = 315/9 = 35$

$c1 = 63 \times (63^{-1} \bmod 5) = 63 \times (3^{-1} \bmod 5) = 63 \times 2 = 126$

$c2 = 45 \times (45^{-1} \bmod 7) = 45 \times (3^{-1} \bmod 7) = 45 \times 5 = 225$

$c3 = 35 \times (35^{-1} \bmod 9) = 35 \times (8^{-1} \bmod 9) = 35 \times 8 = 280$

$X = (1 \times 126 + 2 \times 225 + 3 \times 280) \bmod 315$

$X = (126+450+840) \bmod 315 = 1416 \bmod 315 = 156$

Second Assertion:

It follows from rules for modular arithmetic.

If $A \leftrightarrow (a_1, a_2, ..., a_k)$ and $B \leftrightarrow (b_1, b_2, ..., b_k)$

then

$(A + B) \bmod M \leftrightarrow ((a_1 + b_1) \bmod m_1, ..., (a_k + b_k) \bmod m_k)$

$(A - B) \bmod M \leftrightarrow ((a_1 - b_1) \bmod m_1, ..., (a_k - b_k) \bmod m_k)$

$(A \times B) \bmod M \leftrightarrow ((a_1 \times b_1) \bmod m_1, ..., (a_k \times b_k) \bmod m_k)$

One of the useful features of the Chinese remainder theorem is that it provides a way to manipulate (potentially very large) numbers mod M in terms of tuples of smaller numbers.

Example:

To represent 959 mod 2491 as a pair of numbers mod 47 and 53.

Given: $m_1 = 47$ and $m_2 = 53$ $M = 2491$ $A = 959$

$M_1 = M/m_1 = 2491/47 = 53$
$M_{1_{-1}} = 53_{-1} \bmod 47 = 6_{-1} \bmod 47 = 8 \bmod 47$

$M_2 = M/m_2 = 2491/53 = 47$
$M_{2_{-1}} = 47_{-1} \equiv -9 \equiv 44 \bmod 53$

A1	A2	A3	B1	B2	B3	Q =(A3/B3)
1	0	53	0	1	47	1
0	1	47	1	-1	6	7
1	-1	6	-7	8	5	1
-7	8	5	8	-9	1	

959 is represented as (19, 5) as 959 mod 47 = 19 and 959 mod 53 = 5

To add 648 to 959,

$(648) \leftrightarrow (648 \bmod 47, 648 \bmod 53) = (37, 12)$

$(648+959) \bmod 2491 \leftrightarrow (37+19 \bmod 47, 12+5 \bmod 53) = (9, 17)$

To verify: $(9, 17) \leftrightarrow a_1M_1M_{1_{-1}} + a_2M_2M_{2_{-1}} \bmod M$

$= [(9)(53)(8) + (17)(47)(44)] \bmod 2491$

$= [3816 + 35156] \bmod 2491 = 1607$ $(648+959=1607) \bmod 2491$

MATHEMATICS OF ASYMMETRIC KEY CRYPTOGRAPHY

Order of a (mod n)

If a and n are relatively prime, then there is atleast one integer m that satisfies

$a^m \equiv 1 \pmod n$ m is the smallest positive integer

The order of a modulo n is usually written as $m = ord_n(a)$

Example:

$7^1 \equiv 7 \bmod 19$ $7^2 \equiv 11 \bmod 19$ $7^3 \equiv 1 \bmod 19$

$m = ord_{19}(7) = 3$

The sequence is periodic $7^{3+j} \equiv 7^3 7^j \equiv 7^j \bmod 19$

$7^1 \equiv 7^4 \equiv 7^7 \equiv 7 \bmod 19$ $7^2 \equiv 7^5 \equiv 7^8 \equiv 11 \bmod 19$

Primitive Roots

Any base integer a which generates (via powers) the reduced residue class set modulo n, then such integer a is called as primitive root of modulus n.

If a is a primitive root of n, then its powers a, a^2, a^3, …, $a^{\varphi(n)}$ are distinct (mod n) and are all relatively prime to n. Moreover $a^{\varphi(n)} \equiv 1 \pmod n$

Example 1: 6 is primitive root of 11

$6^1 \equiv 6 \bmod 11$ $6^4 \equiv 9 \bmod 11$ $6^7 \equiv 8 \bmod 11$ $6^{10} \equiv 1 \bmod 11$

$6^2 \equiv 3 \bmod 11$ $6^5 \equiv 10 \bmod 11$ $6^8 \equiv 4 \bmod 11$

$6^3 \equiv 7 \bmod 11$ $6^6 \equiv 5 \bmod 11$ $6^9 \equiv 2 \bmod 11$

Reduced Residue Set of 11 = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}

Example 2: 3 is primitive root of 10

$3^1 \equiv 3 \bmod 10$ $3^2 \equiv 9 \bmod 10$ $3^3 \equiv 7 \bmod 10$ $3^4 \equiv 1 \bmod 10$

Reduced Residue Set of 10 = {1, 3, 7, 9}

- The integers having primitive roots are 2, 4, p^n and $2p^n$, where p is any odd prime and n is a positive integer.
- The number of primitive roots modulo n, if there are any, is equal to ϕ ($\phi(n)$)

Example: To check whether 6 is primitive root of 11

$\phi(n) = \phi(11) = 10 = 2.5$ (prime factors)

Test a=6:

$6^{10/5} = 6^2 \equiv 36 \equiv 3 \not\equiv 1 \bmod 11$

$6^{10/2} = 6^5 \equiv 3.3.6 \equiv 10 \not\equiv 1 \bmod 11$

6 is primitive root of 11

Discrete Logarithms (Index)

$b \equiv a^i \pmod p$ where $0 \le i \le (p-1)$

This exponent i is referred to as the discrete logarithm of the number b for the base a (mod p). This value is denoted as $\text{dlog}_{a,p}(b)$.

$\text{dlog}_{a,p}(1) = 0$ because $a^0 \bmod p = 1 \bmod p = 1$

$\text{dlog}_{a,p}(b) = 1$ because $a^1 \bmod p = b$

Methods to compute discrete logarithms:

- The Pohlig-Hellman Algorithm
- Baby Step, Giant Step
- The Index Calculus

Example:

$\text{dlog}_{2,11}(7) = ?$ Finding i such that $2^i \bmod 11 = 7$

Using Brute-force method:

$2 \bmod 11 = 2$ $2^2 \bmod 11 = 4$ $2^7 \bmod 11 = 7$

$2^3 \bmod 11 = 8$ $2^4 \bmod 11 = 5$

$2^5 \bmod 11 = 10$ $2^6 \bmod 11 = 9$

b	2	4	8	5	10	9	7
$\text{dlog}_{2,11}(b)$	1	2	3	4	5	6	7

Even though discrete logarithms is not a one-way trap-door function, it is a hard problem. That is, it is infeasible to compute discrete logarithms.

ASYMMETRIC KEY CIPHERS

RSA

RSA was developed by Ron Rivest, Adi Shamir, and Len Adleman at MIT in 1977.

It is a public-key cryptographic algorithm.

The RSA scheme is a block cipher in which the plaintext and ciphertext are integers between 0 and n - 1 for some n.

A typical size for n is 1024 bits, or 309 decimal digits.

Applications of RSA

Key Exchange in TLS, WTLS etc.

Producing Digital Signatures in SSL Certificate, PGP, S/MIME etc.

Encrypting Symmetric Keys in PGP, S/MIME etc.

Algorithm Description

Let Plaintext block - M, Ciphertext block - C

$C = M^e \bmod n$

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

Both sender and receiver must know the value of n.

Sender knows the value of e and only receiver knows the value of d.

Public Key PU = {e, n}

Private Key PR = {d, n}

For this algorithm to be satisfactory for public-key encryption, the following requirements must be met.

1. It is possible to find values of e, d, n such that $M^{ed} \bmod n = M$ for all $M < n$.
2. It is relatively easy to calculate $M^e \bmod n$ and $C^d \bmod n$ for all values of $M < n$.

3.It is infeasible to determine d given e and n.

$\phi(n) = \phi(pq) = \phi(p)\,\phi(q) = (p-1)(q-1)$

$ed \bmod \phi(n) = 1$

$ed \equiv 1 \bmod \phi(n)$

$d \equiv e^{-1} \bmod \phi(n)$

ASYMMETRIC KEY CIPHERS

RSA Algorithm

User B (Receiver):

1. Select p,q p and q both prime, $p \neq q$
2. Calculate $n = p * q$
3. Calculate $\phi(n) = (p - 1)(q - 1)$
4. Select integer e, $\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
5. Calculated d $d \equiv e^{-1} \bmod \phi(n)$

Public key PU = {e, n} Private key PR = {d, n}

Encryption by User A (Sender) with User B's Public Key:

Plaintext: $M < n$

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

Decryption by User B (Receiver) with User B's Private Key:

Ciphertext: C

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

Decryption using CRT

$M = C^d \bmod n$

$V_p = C^d \bmod p$ $V_q = C^d \bmod q$

$V_p = C^{d \bmod (p-1)} \bmod p$ $V_q = C^{d \bmod (q-1)} \bmod q$

$X_p = q \times (q^{-1} \bmod p)$ $X_q = p \times (p^{-1} \bmod q)$

$M = (V_pX_p + V_qX_q) \bmod n$

Fast Modular Exponentiation: To compute $a^b \bmod n$ quickly

Example: $2^{560} \bmod 561 = 1$ (final value of f in the below table)

Initial value of f = 1, a=2, n = 561, b = 560 = $(1000110000)_2$

f = (f × f) mod n	1	4	16	256	460	412	166	67	1	**1**
B_i	1	0	0	0	1	1	0	0	0	0
f = (f × a) mod n	2	-	-	-	359	263	-	-	-	-

ASYMMETRIC KEY CIPHERS

#Problem: Perform encryption and decryption for the parameters

p=3, q=11, e=7, M=5

Solution:

Encryption

$C = M^e \bmod n$

$n = p \times q = 3 \times 11 = 33$

$C = 5^7 \bmod 33$

$5^3 = 125 \equiv 26 \bmod 33$

$5^6 \equiv 676 \equiv 16 \bmod 33$

$5^7 \equiv 16.5 \equiv 80 \equiv 14 \bmod 33$

$C = 14$

Decryption

$M = C^d \bmod n$

$\phi(n) = (p - 1)(q - 1) = 2.10 = 20$

$d \equiv e^{-1} \bmod \phi(n) \Rightarrow d \equiv 7^{-1} \bmod 20 \Rightarrow d=3$

$M = 14^3 \bmod 33$

$14^2 = 196 \equiv 31 \bmod 33$ $\quad$ $14^3 \equiv 31.14 \equiv 434 \equiv 5 \bmod 33$

$M = 5$

Decryption Using CRT

C=14, p=3, q=11 n=33

$V_p = C^{d \bmod (p-1)} \bmod p$ $\quad$ $V_q = C^{d \bmod (q-1)} \bmod q$

$V_p = 14^{3 \bmod 2} \bmod 3$ $\quad$ $V_q = 14^{3 \bmod 10} \bmod 11$

$V_p = 14 \bmod 3 = 2$ $\quad$ $V_q = 14^3 \bmod 11 \equiv 3^3 \bmod 11 = 5$

$X_p = 11 \times (11^{-1} \bmod 3)$ $\quad$ $X_q = 3 \times (3^{-1} \bmod 11)$

$X_p = 11 \times (2^{-1} \bmod 3) = 11 \times 2 = 22$ $\quad$ $X_q = 3 \times (3^{-1} \bmod 11) = 3 \times 4 = 12$

$M = (V_pX_p + V_qX_q) \bmod n = (2.22 + 5.12) \bmod 33 = (44+60) \bmod 33 = 5$

$M = 5$

ASYMMETRIC KEY CIPHERS

Security of RSA

❖ Brute force

This involves trying all possible private keys.

❖ Mathematical attacks

There are several approaches, all equivalent in effort to factoring the product of two primes.

❖ Timing attacks

- These depend on the running time of the decryption algorithm.
- Countermeasures to prevent timing attacks are (i) Constant exponentiation time, (ii) Random delay, and (iii) Blinding

❖ Chosen ciphertext attacks

❖ This type of attack exploits properties of the RSA algorithm.

Factoring Algorithms:

❖ Pollard's p-1 algorithm

❖ Pollard's rho algorithm

❖ Elliptic Curve Factorization Method (ECM)

❖ Quadratic Sieve: It is fastest method for factoring integers less than 110 digits.

❖ Generalized number field sieve: It is the most efficient method for factoring integers larger than 110 digits.

Generalized number field sieve and Quadratic sieve are the fastest algorithms and hence mostly used for performing mathematical attacks on RSA.

Key Distribution

Keys distribution can be categorized into public key distribution and secret key distribution.

To distribute public keys there are various schemes like

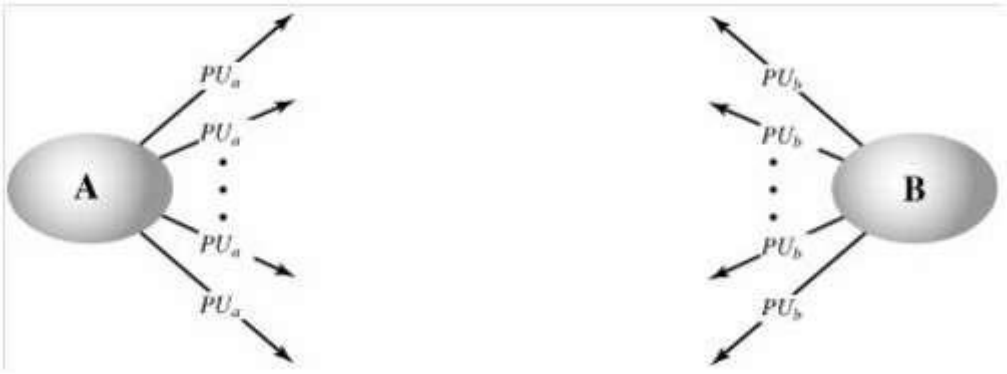
1.Public announcement

2.Publicly available directory

3.Public key authority

4. Public key certificates

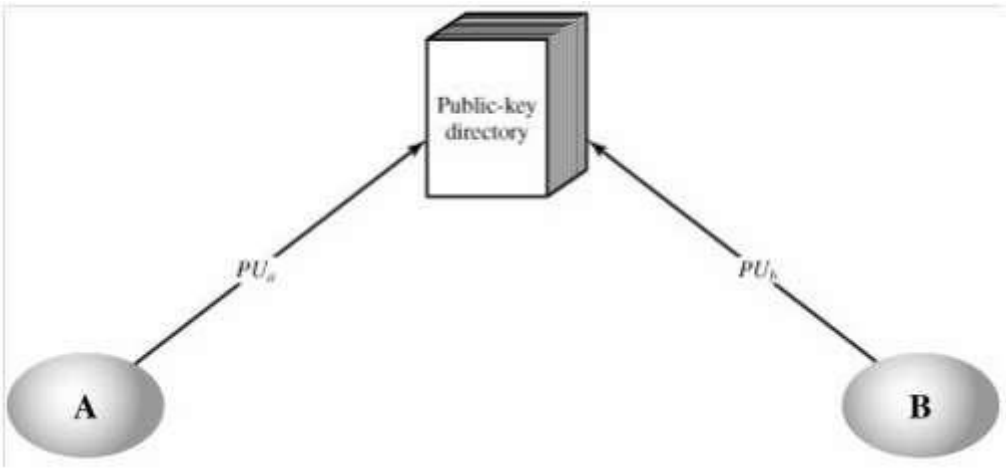
Public Announcement of Public Keys



In this distribution scheme the public keys are broadcasted to the large community. The limitation in this public announcement is that anyone can announce the key. Similarly a person A can pretend to be another person B and can publicly announce a public key for that user B. So when all users are sending the messages encrypted using the public key of user B it is actually can be decrypted only by user A.

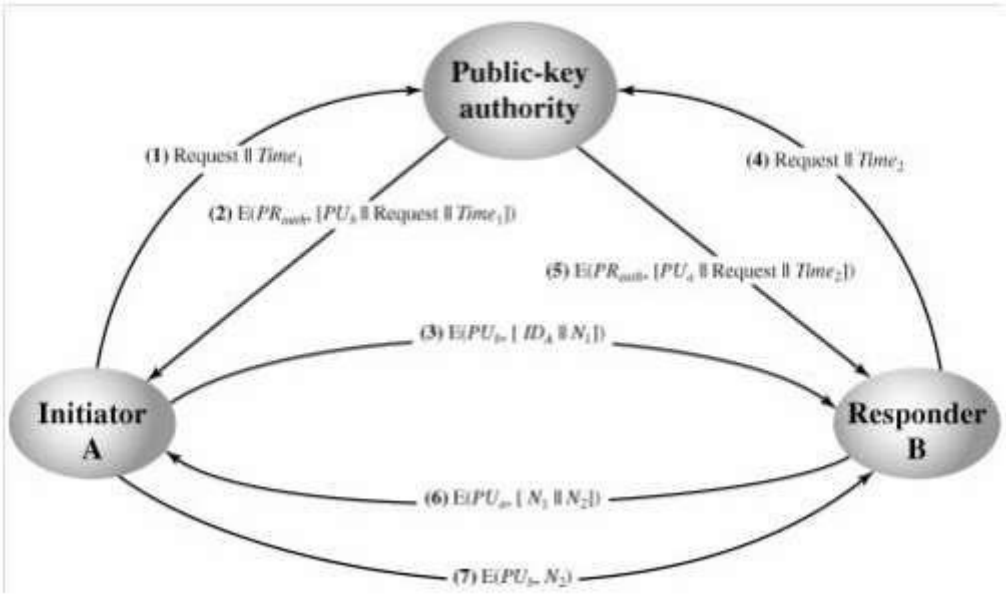
Publicly Available Directory

To overcome the drawback of the public announcement all users can share their public keys to the public directory which is maintained by an authority. Initially all users has to register in this public directory and each user is authenticated by the authority to access the public directory. So, it is not possible to perform masquerade attack. i.e., user A cannot send another person B's key. At any point of time the keys can be replaced by the concerned user. This scheme also has a drawback that an adversary can compromise the private key shared between the user and public authority.



Public-Key Authority

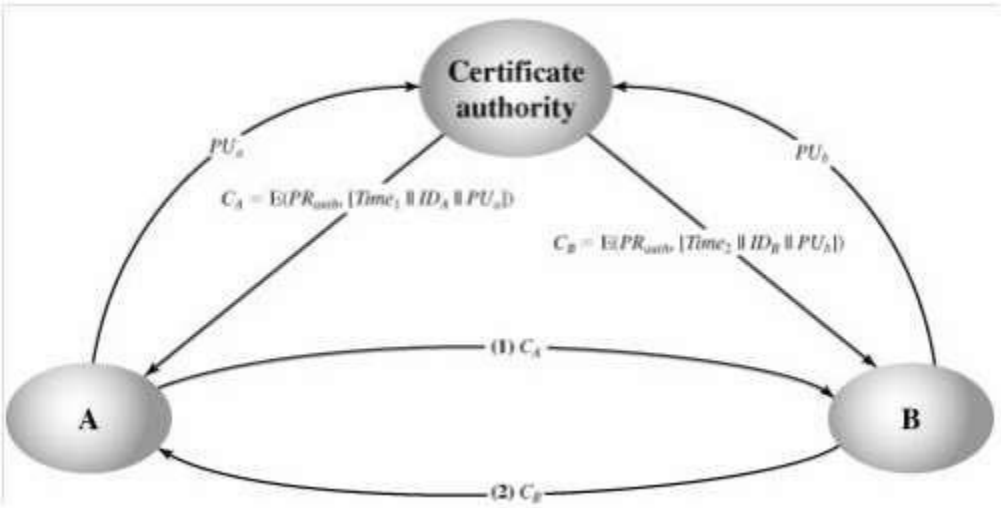
To avoid the weakness in the public directory scheme, each participant has to request the public authority for user B's public key by sending a time stamped request message. After receiving the request message, public key authority sends a response as encrypted message to the user A. Encryption is done using authority's private key which authenticates that the message is sent by the authority. Encrypted message has B's public key, and the user A's request message. Now if A wants to communicate with user B , user A will send an encrypted message to user B with a nonce and identifier of user A.



After receiving user B will send the reply as an encrypted message with the nonce sent by A and a new nonce value to uniquely identify the communication and to make an assurance that user B has received the message correctly. Later A will also send the new nonce value encrypted to make an assurance that both intended users are only communicating.

Public-Key Certificates

In the public key authority, as each user has to contact authority in-order to get the public keys. So bottleneck problem occurs. To avoid this issue each user will share the public key to the central authority who is responsible for issuing certificates to the users. Each user will be provided with certificate. So if any user wants to communicate they will exchange the certificates to authenticate themselves. Certificate will have users public key and the central authority's private key.



Each certificate has

CA = E(PRauth, [T||IDA||PUa])

where PRauth is the private key used by the authority and T is a timestamp.

This certificate can be verified by performing

D(PUauth, CA) = D(PUauth, E(PRauth, [T||IDA||PUa])) = (T||IDA||PUa)

DIFFIE HELLMAN KEY EXCHANGE

Whittfield Diffie and Martin Hellman are called the inventors of public key cryptography.

Diffie Hellman key exchange is the first public key algorithm published in 1976. Diffie Hellman is a public key algorithm. It only used for key exchange. Does not used for encryption and decryption. It is based on discrete logarithm. It is widely used in security protocols and commercial products.

Primitive roots

Let 'P' be a prime then 'b' is a primitive root for P if the powers of b, 1, b, b2 , b3…. by including all of the residue classes mod P except 0. Hence there must be P – 1 power of b.

Example 1:

If P = 7, then 3 is a primitive root for P because the power of 3 are 1, 3, 2, 6, 4, 5.

1, 3, 32, 33, 34 , …

1, 3, 9 mod 7, 27 mod 7, 31 mod 7

1, 3, 2, 6, 4, 5.

Example 2:

If P = 13, then 2 is a primitive root for P because the power of 2 are

1, 2, 22, 23, 24 , 25 , 26 , …

1, 2, 4 mod 13, 8 mod 13, 16 mod 13, 32 mod 13m 128 mod 13, 256 mod 13

1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7

Diffie Hellman Algorithm

Let 'q ' be a prime.

Given α where $\alpha < q$ and α ιs a primitive root of q.

User 'A' key generation

Select prime key XA where XA < q.

Calculate public key YA where $YA = \alpha^{XA} \bmod q$.

User 'B' generation

Select private key XB where XB < q.

Calculate public key YB where $YB = \alpha^{XB} \bmod q$.

Generation of secret key by user 'A'

$K = (YB)^{XA} \bmod q$

Generation of secret key by user 'B'

$K = (YA)^{XB} \bmod q$

Derivation

$K = (YB)^{XA} \bmod q$

$= (\alpha^{XB} \bmod q)\ XA \bmod q$

$= (\alpha^{XB})^{XA} \bmod q$

$= (\alpha^{XA})^{XB} \bmod q$

$= (\alpha^{XA} \bmod q)^{XB} \bmod q$

$K = (YA)^{XB} \bmod q$

Elliptic Curve Cryptography

A major issue with the use of Public-Key Cryptography, is the size of numbers used, and hence keys being stored. Recently, an alternate approach has emerged, elliptic curve cryptography (ECC), which performs the computations using elliptic curve arithmetic instead of integer or polynomial arithmetic.

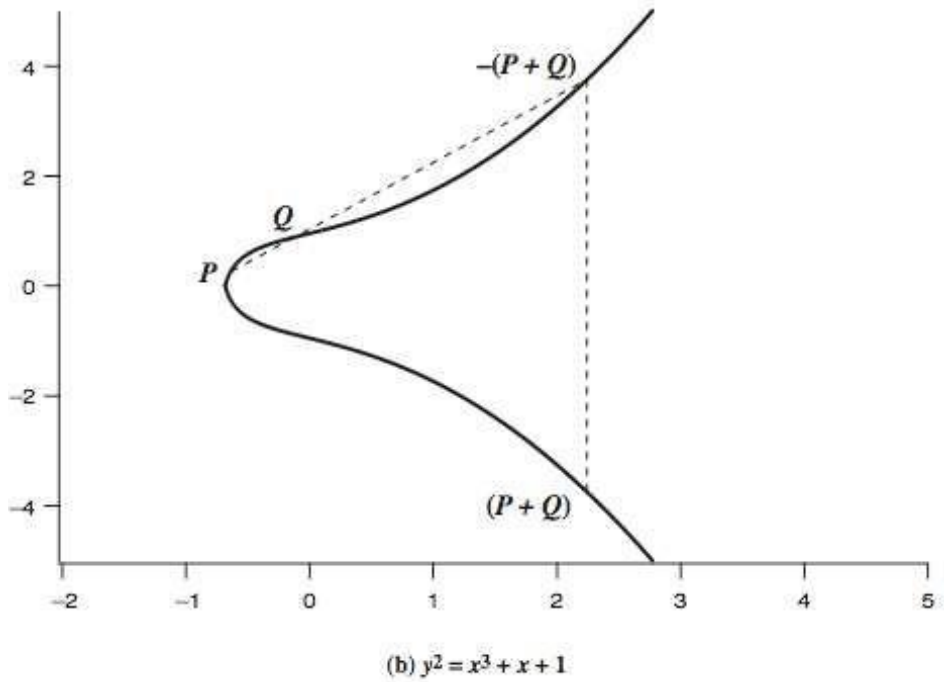
The principal attraction of ECC, compared to RSA, is that it appears to offer equal security for a far smaller key size, thereby reducing processing overhead.

Elliptic Curve

An elliptic curve is defined by an equation in two variables with coefficients. In general, cubic equations for elliptic curves take the following form, known as a Weierstrass equation:

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

where a, b, c, d, e are real numbers and x and y take on values in the real numbers.



(b) $y^2 = x^3 + x + 1$

Figure Example of Elliptic Curves

For our purpose, it is sufficient to limit ourselves to equations of the form

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

- where x,y,a,b are all real numbers, also define zero point O

➢ consider set of points E(a,b) that satisfy

➢ have addition operation for elliptic curve

- geometrically sum of P+Q is reflection of the intersection R

If three points on an elliptic curve lie on a straight line, their sum is O. hence define addition as:

1. O serves as the additive identity. Thus O = –O; for any point P on the elliptic curve, P + O = P. In what follows, we assume P <> O and Q <> O.
2. The negative of a point P is the point with the same x coordinate but the negative of the y coordinate; that is, if P = (x, y), then –P = (x, –y). These two points can be joined by a vertical line & that P + (–P) = P – P = O.

1. To add two points P and Q with different x coordinates, draw a straight line between them and find the third point of intersection R. There is a unique point R that is the point of intersection (unless the line is tangent to the curve at either P or Q, in which case we take R = P or R = Q, respectively). To form a group structure, we need to define addition on these three points as follows: P + Q = – R. ie. P + Q to be the mirror image (with respect to the x axis) of the third point of intersection as shown on slide.

2. The geometric interpretation of the preceding item also applies to two points, P and –P, with the same x coordinate. The points are joined by a vertical line, which can be viewed as also intersecting the curve at the infinity point. We therefore have P + (–P) = O, consistent with item (2).

3. To double a point Q, draw the tangent line and find the other point of intersection S. Then Q + Q = 2Q = –S.

2. With the preceding list of rules, it can be shown that the set E(a, b) is an abelian group.

Elliptic curve arithmetic

Addition of Two Points

Let the points P = (x_1, y_1) and Q= (x_2, y_2) be in the elliptic group E_p (a, b), and O is the point at infinity. The rules for addition over the elliptic group E_p (a, b) are:

P+O=O+P=P

If x2= x1 and y2 = -y1, that is P = (x1, y1) and Q= (x2, y2)= (x_1, $-y_1$) = –P, then P+Q=O.

If Q = –P, then the sum P+Q = (x_3, y_3) is

given by: $x_3 = \lambda^2 - x_1 - x_2 \bmod p$

$y_3 = \lambda (x_1 - x_3) - y_1 \bmod p$

Where

$$\lambda \triangleq \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{if } P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1}, & \text{if } P = Q \end{cases}$$

Subtraction of Two Points

Let the points P = (x1, y1) and Q = (x2, y2) be in the elliptic group Ep (a, b). The rules for subtraction over the elliptic group Ep (a, b) are:

P–Q=P+(–Q)=P+(inverse of Q), so the inverse of Q is Q(x2, y2)= Q(x2, -y2)

= Q(x2, p-y2).

Multiplication Points by a Constant

Let the points P = (x1, y1) and the integer be k in the elliptic group Ep (a, b). Then Pk= Add P with k times. e.g., 2P = P+P = (x1, y1) + (x1, y1) = (x3, y3).

Point generation on Elliptic Curve

Let P = (3,10) ∈E23(1,1). Then 2P = (x3, y3) is equal to: 2P = P + P = (x1, y1) + (x1, y1) Since P=Q and x2 = x1, the values of λ, x3 and y3 are given by:

$$\lambda = \frac{3x_1^2 + a}{2y_1} \bmod p = \frac{3 \times 3^2 + 1}{2 \times 10} \bmod 23$$

$$= \frac{5}{20} \bmod 23 = 4^{-1} \bmod 23$$

Now using extended Euclidean formula: Here, quotient = q, remainder = r and $t = t_1 - qt_2$

Q	r_1	r_2	R	t_1	t_2	t
5	23	4	3	0	1	**-5**
1	4	3	1	1	-5	**6**
3	3	1	0	-5	6	**-23**
	1	**0**		**6**	**-23**	

Since, $r_1 = 1$. So that, $M_{1\text{-}1} = t_1$. The extended Euclidean Algorithm gives $t_1 = 6$. So, the multiplicative inverse (M^{-1}) is 6 mod 23 =6.

$x_3 = {}^2 - x_1 - x_2 = 6^2 - 3 - 3 \bmod 23 = 30 \bmod 23 = 7$

$y_3 = (x_1 - x_3) - y_1 = 6 \times (3-7) - 10 \bmod 23 = -34 \bmod 23 = 12$

Therefore $2P = (x_3, y_3) = (7, 12)$.

The multiplication kP is obtained by doing the elliptic curve addition operation k times by following the same additive rules.

ECC Diffie-Hellman

The elliptic curve analog of Diffie-Hellman key exchange, which is a close analogy given elliptic curve multiplication equates to modulo exponentiation. Key exchange using elliptic curves can be done in the following manner.

First pick a large integer q, which is either a prime number p or an integer of the form 2^m and elliptic curve parameters a and b for Equation

$$y^2 \bmod p = (x^3 + ax + b) \bmod p$$

This defines the elliptic group of points $E_q(a, b)$. Next, pick a base point $G = (x_1, y_1)$ in $E_q(a, b)$ whose order is a very large value n. The order n of a point G on an elliptic curve is the smallest positive integer n such that $nG = O$. So $E_q(a, b)$ and G are parameters of the cryptosystem known to all participants. A key exchange between users A and B can then be accomplished as shown. To break this scheme, an attacker would need to be able to compute k given G and kG, which is assumed hard.

A key exchange between users A and B can be accomplished as follows

1. A selects an integer nA less than n. This is A's private key. A then generates a public key $P_A = n_A * G$; the public key is a point in Eq(a, b).
2. B similarly selects a private key n_B and computes a public key P_B.
3. A generates the secret key $k = n_A * P_B$. B generates the secret key

   $k = n_B * P_A$.

The two calculations in step 3 produce the same result because

$$n_A * P_B = n_A * (n_B * G) = n_B * (n_A * G) = n_B * P_A$$

To break this scheme, an attacker would need to be able to compute k given G and kG, which is assumed to be hard.As an example,6 take p = 211; Ep(0,-4), which is equivalent to the curve y2 = x3 - 4; and G = (2, 2). One can calculate that 240G = O.

- A's private key is $n_A = 121$, so A's public key is $P_A = 121(2, 2) = (115, 48)$.
- B's private key is $n_B = 203$, so B's public key is $203(2, 3) = (130, 203)$.
- The shared secret key is $121(130, 203) = 203(115, 48) = (161, 69)$.

ECC Encryption/Decryption

Several approaches to encryption/decryption using elliptic curves have been analyzed in the literature. This one is an analog of the ElGamal public-key encryption algorithm. The sender must first encode any message M as a point on the elliptic curve P_m. Note that the ciphertext is a pair of points on the elliptic curve. The sender masks the message using random k, but also sends along a "clue" allowing the receiver who know the private-key to recover k and hence the message. For an attacker to recover the message, the attacker would have to compute k given G and kG, which is assumed hard.

Key Generation:

- Each user chooses private key $n_A<n$
- compute public key $P_A=n_AG$

Encryption:

- P_m : $C_m=\{kG, P_m+kP_b\}$, k random

Decryption:

C_m compute:

- $P_m+kP_b–n_B(kG) = P_m+k(n_BG)–n_B(kG) = P_m$

Let us consider a simple example. The global public elements are q = 257;

Eq(a, b) = $E_{257}(0, -4)$, which is equivalent to the curve $y^2 = x^3 - 4$; and G =(2, 2).

- Bob's private key is n_B = 101, and his public key is

$$P_B = n_BG = 101(2, 2)$$

$$= (197, 167).$$

- Alice wishes to send a message to Bob that is encoded in the elliptic point

P_m = (112, 26).

- Alice chooses random integer k = 41 and computes kG =41(2, 2) = (136, 128),

  $kP_B = 41(197, 167) = (68, 84)$

  $P_m + kP_B = (112, 26)+ (68, 84) = (246, 174).$

- Alice sends the ciphertext

  $C_m = (C_1, C_2) = \{(136, 128),(246, 174)\}$ to Bob.

- Bob receives the ciphertext and computes

  $C_2 - n_BC_1 = (246, 174) - 101(136, 128)$

  $= (246, 174) - (68, 84)$

  $= (112, 26).$

ECC Security

The security of ECC depends on how difficult it is to determine k given kP and P. This is referred to as the elliptic curve logarithm problem. The fastest known technique for taking the elliptic curve logarithm is known as the Pollard rho method. Compared to factoring integers or polynomials, can use much smaller numbers for equivalent levels of security. Comparable Key Sizes for Equivalent Security shown in below table:

Symmetric scheme (key size in bits)	ECC-based scheme (size of n in bits)	RSA/DSA (modulus size in bits)
56	112	512
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360

ASSIGNMENT UNIT III

S.No	Questions	CO	K
SET 1			
1.	Six professors begin courses on Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday, respectively, and announce their intentions of lecturing at intervals of 2, 3, 4, 1, 6, and 5 days, respectively. The regulations of the university forbid Sunday lectures (so that a Sunday lecture must be omitted). When first will all six professors find themselves compelled to omit a lecture? (Use CRT).	co3	K3
2.	Using Elliptic curve encryption/decryption scheme, key exchange between users A and B is accomplished. The cryptosystem parameters are, elliptic group of points $E_{11}(1,6)$ and point G on the elliptic curve is G=(2,7). B's secret key is $n_B=7$. Now when (i)A wishes to encrypt the message $P_m=(10,9)$ and chooses the random value K=3. Determine the ciphertext C_m. (ii) How will B recover P_m from C_m. (iii) Find out B's public key P_B.	co3	K3
SET 2			
3.	Using the RSA scheme, let p = 809, q = 751, and d= 23. Calculate the public key e. Then Sign and Verify a message with M_1=100. Call the signature S_1. Sign and Verify a message with M_2=50. Call the signature S_2. Show that if M=M_1×M_2=5000, then S= S_1×S_2.	co3	K3
4.	Users A and B use the Diffie-Hellman key exchange technique, a common prime p=71 and a primitive root g=7 are used. If user A has private key $X_A=5$, what is A's public key Y_A? If user B has private key $X_B=12$, what is B's public key Y_B? What is the shared secret key?	co3	K3

ASSIGNMENT UNIT III

S.No	Questions	CO	K
SET 3			
5.	Solve the simultaneous congruences $x \equiv 6 \pmod{11}$, $x \equiv 13 \pmod{16}$, $x \equiv 9 \pmod{21}$, $x \equiv 19 \pmod{25}$.	co3	K3
6.	Perform encryption and decryption using the RSA algorithm for the following: p = 17; q = 31, e = 7;M = 2. Use CRT for decryption.	co3	K3
SET 4			
7.	In a public key cryptosystem using RSA algorithm, you catch the cipher text 11 and send to a user whose public key is (7, 187). What is the plain text message?	co3	K3
8.	For the given simultaneous linear congruences: $X \equiv 2 \pmod{3}$ $X \equiv 3 \pmod{5}$ $X \equiv 2 \pmod{7}$	co3	K3
SET 5			
9.	Find the last 3 digits of 7^{403}	co3	K3
10.	Using Fermat's theorem, find $3^{201} \bmod 11$	co3	K3

TWO MARKS Q & A

Define one-way function. (CO3, K1)

A one-way function is one that maps a domain into a range such that every function value has a unique inverse, with the condition that the calculation of the function is easy whereas the calculation of the inverse is infeasible:

$Y = f(X)$ easy

$X = f^{-1}(Y)$ infeasible

Define trap-door one-way function. (CO3, K1)

It is one that is easy to calculate in one direction and infeasible to calculate in the other direction unless certain additional information is known. With the additional information the inverse can be calculated in polynomial time.

$Y = f_k(X)$ easy, if k and X are known

$X = f^{-1}_k(Y)$ easy, if k and Y are known

$X = f^{-1}_k(Y)$ infeasible, if Y is known but k is not known

Compare secret key and public key cryptography. (CO3, K2)

S.No.	Secret Key Cryptography	Public Key Cryptography
1	The key is shared between sender and receiver. It is not known to others.	Private key of b user is known only to that user. Public key of b user is known to group of users.
2	Encryption and decryption algorithms use same key. Hence it is known bs symmetric key encryption.	Encryption and decryption algorithms use different keys. Hence it is known as asymmetric key encryption.

State Fermat's theorem. (CO3, K1)

If p is prime and a is a positive integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$.

Example: $7^{18} \equiv 1 \pmod{19}$

Define Euler's totient function. (CO3, K1)

It is defined as the number of positive integers less than n and relatively prime to n. It is denoted by φ (n). Example: φ (11) = 10, φ (10) = 4

State Euler's theorem. (CO3, K1)

If b and n are relatively prime, then $a^{\varphi(n)} \equiv 1 \pmod{n}$. Example: $13^8 \equiv 1 \pmod{20}$

Define primitive roots. (CO3, K1)

If a is a primitive root of n, then its powers a, a^2, a^3, …, $a^{\varphi(n)}$ are distinct (mod n) and are all relatively prime to n. Moreover $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Define discrete logarithm. (CO3, K1)

$$b \equiv a^i \pmod{p} \text{ where } 0 \leq i \leq (p-1)$$

This exponent i is referred to as the discrete logarithm of the number b for the base a (mod p). This value is denoted as $\text{dlog}_{a,p}(b)$.

The Miller-Rabin test can determine if a number is not prime but cannot determine if a number is prime. How can such an algorithm be used to test for primality? (CO3, K2)

If the number of Miller-Rabin tests t=1, the probability that a nonprime number will pass the test is less than 0.25. If the number of tests increased to t=10, then probability that a nonprime number will pass all ten tests is less than 10^{-6}. In general getting false positive is $(1/4)^t$. So by choosing t different value of a, one can close to 100% confidently determine a number as prime.

List out the three broad categories of applications of public-key cryptosystems. (CO3, K2)

- Encryption and decryption
- Digital Signature
- Key Exchange

How is authentication and confidentiality achieved by asymmetric encryption system? (CO3, K2)

- Confidentiality is achieved when the sender encrypts the message with the recipient's public key.
- Authentication is achieved when the sender signs a message with its (sender's) private key.

What is the idea behind the security of RSA?

The security of RSA lies in the fact that Integer Factorization (factoring an integer into their prime factors) is hard.

List out the different primality-testing algorithms. (CO3, K2)

- Fermat primality test
- Miller-Rabin primality test
- Solovay-Strassen primality test

List out the different types of attacks on RSA? (CO3, K2)

- Low Exponent attack
- Short plaintext attack
- Timing attack
- Mathematical attack (Factoring)

List out the different factorization algorithms.

- ❖ Quadratic Sieve
- ❖ Generalized number field sieve
- ❖ Elliptic Curve Factorization Method (ECM)

Define man-in-the middle-attack. (CO3, K1)

An attacker interposes during key exchange, acting as the client to the server and as the server to the client. This attack involves persuading the client and server to believe that they are talking to each other when in fact the communication is going through an intermediate attacker.

Define an elliptic curve. (CO3, K1)

An elliptic curve is defined by an equation in two variables with coefficients. For cryptography, the variables and coefficients are restricted to elements in a finite field.

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

Perform encryption and decryption using RSA Alg. for the following. P=7; q=11; e=17;M=8.

n = pq

n = 7*11=77

Φ(n)=(p-1) (q-1)

=6*10 = 60

e =17 d =27

C = M^e mod n

C = 817 mod 77

= 57

M = Cd mod n

= 5727 mod 77 = 8

Specify the applications of the public key cryptosystem?

The applications of the public-key cryptosystem can classified as follows

Encryption/Decryption: The sender encrypts a message with the recipient's public key.

Digital signature: The sender "signs" a message with its private key. Signing is achieved by a cryptographic algorithm applied to a message or to a small block of data that is a function of the message.

Key Exchange: Two sides cooperate to exchange a session key. Several different approaches are possible, involving the private key(s) of one or both parties.

List four general characteristics of schema for the distribution of the public key?

The four general characteristics for the distribution of the public key are

Public announcement

Publicly available directory

Public-key authority

Public-key certificate

What is a public key certificate?

The public key certificate is that used by participants to exchange keys without contacting a public key authority, in a way that is as reliable as if the keys were obtained directly from the public-key authority. Each certificate contains a public key and other information, is created by a certificate authority, and is given to a participant with the matching private key.

What is key distribution center?

A key distribution center is responsible for distributing keys to pairs of users such as hosts, processes, applications. Each user must share a unique key with the key distribution center for purposes of key distribution.

List out the attacks to RSA.

Brute force - Trying all possible private keys.

Mathematical attacks - The approaches to factor the product of two prime numbers.

Timing attack - Depends on the running time of the decryption algorithm.

PART B

1.Users Alice and Bob use the Diffie Hellman key exchange technique with common prime q = 83 and primitive root α = 5.

(i) If Alice has a private key as 6, what is public key of Alice?

(ii) If Bob has a private key as 10 , what is the public key of Bob?

(iii) What is the shared secret key?

2.Users A and B use the Diffie-Hellman key exchange technique, a common prime p=71 and a primitive root g=7 are used. If user A has private key X A =5, what is A's public key Y A ? If user B has private key X B =12, what is B's public key Y B ? What is the shared secret key? Explain briefly about man-in-the-middle man attack.

3.Find the secret key shared between user A and user B using Diffie Hellman algorithm for the following q=353 , α = 3, X A = 45 and X B = 50

4. Explain ElGamal Cryptosystem

5. Explain key distribution techniques.

6. Using Elliptic curve encryption/decryption scheme, key exchange between users A and B is accomplished. The cryptosystem parameters are, elliptic group of points E 11 (1,6) and point G on the elliptic curve is G=(2,7). B's secret key is n B =7. Now when (i) A wishes to encrypt the message Pm=(10,9) and chooses the random value K=3. Determine the ciphertext Cm. Find out B's public key PB.

7.State Chinese Remainder Theorem and find X for the given set of congruent equations using CRT

$X \equiv 1 \pmod 5$

$X \equiv 2 \pmod 7$

$X \equiv 3 \pmod 9$

$X \equiv 4 \pmod{11}$

8.Perform encryption and decryption using RSA algorithm. Given: p=5; q=11; e=3; M=9.Explain the strength of RSA.

GATE QUESTIONS

1. RSA Cryptosystem – GATE CSE 2019

Question:
In an RSA cryptosystem, the value of the public modulus parameter n is 3007. If it is also known that (n)=2880, where ϕ denotes Euler's Totient Function, then the prime factor of n which is greater than 50 is _____.

Answer: 97

Explanation:
Given n=3007 and ϕ(n)=2880. Since n=p×q and ϕ(n)=(p−1)(q−1), we can factor n to find its prime factors. Testing for divisibility, we find 3007=31×97. Among these, the prime factor greater than 50 is 97.

2. RSA Cryptosystem – GATE CSE 2017

Question:
In an RSA cryptosystem, a participant A uses two prime numbers p=13 and q=17 to generate her public and private keys. If the public key of A is 35, then the private key of A is _____.
Answer: 11
Explanation:
Compute n=p×q=13×17=221 and ϕ(n)=(p−1)(q−1)=12×16=192. The private key d is the modular multiplicative inverse of e=35 modulo ϕ(n)=192. Solving $35 \times d \equiv 1 \bmod 192$, we find d=11.

3. Diffie-Hellman Key Exchange – GATE CSE 2005

Question:
Suppose that two parties A and B wish to set up a common secret key (D-H key) between themselves using the Diffie-Hellman key exchange technique. They agree on 7 as the modulus and 3 as the primitive root. Party A chooses 2 and party B chooses 5 as their respective secrets. Their D-H key is:
Options:
A. 3
B. 4
C. 5
D. 6
Answer: B. 4
Explanation:
Public parameters: modulus p=, base g=3. Private keys: A chooses a=2, B chooses b=5. A computes $A = g^a \bmod p = 32 \bmod 7 = 2$, B computes $B = g^b \bmod p = 35 \bmod 7 = 5$. Shared secret: A computes $s = B^a \bmod p = 52 \bmod 7 = 4$, B computes $s = A^b \bmod p = 25 \bmod 7 = 4$. So, the shared key is 4.

4. Euler's Totient Function – GATE CSE 2005

Question:

If ϕ is Euler's Totient function, then $\phi(92)=$ _____.

Answer: 44

Explanation:

The prime factorization of 92 is 22×23. Euler's Totient function $\phi(n)$ for $n=pa\times qb$ is $\phi(n)=n\times(1-(1/p))\times(1-(1/q))$. Thus,

$\phi(92)=92\times(1-(1/2))\times(1-(1/23))=92\times(1/2)\times(22/23)=44$.

5. Chinese Remainder Theorem – GATE CSE 2007

Question:

Find the smallest positive integer x such that:

$x\equiv3 \mod 5$

$x\equiv4 \mod 7$

Answer: 24

Explanation:

Using the Chinese Remainder Theorem, we can find a unique solution modulo $5\times7=35$. Solving the congruences, we find $x=24$ satisfies both conditions.

6.Primality Testing – GATE CSE 2013

Question:

Which of the following numbers is a prime?

Options:

A. 91

B. 97

C. 111

D. 143

Answer: B. 97

Explanation:

Among the options, 97 is a prime number. The others can be factored:

$91 = 7 \times 13$

$111 = 3 \times 37$

$143 = 11 \times 13$

7. Fermat's Theorem – GATE CSE 2019

The value of 351 mod 5 is_____.

Answer

Correct answer is 2

10. Primality Testing – GATE CSE 2013

Which of the following is a probabilistic primality test?

A. Trial Division

B. AKS Primality Test

C. Fermat Primality Test

D. Sieve of Eratosthenes

Answer: C. Fermat Primality Test

Explanation: The Fermat Primality Test is a probabilistic method that can identify composite numbers but may falsely identify some composites (Carmichael numbers) as primes.

Supportive online Certification courses

NPTEL

- Cyber Security and Privacy
- Ethical Hacking
- Computational number theory and cryptography

COURSERA

- Cryptography
- Applied Cryptography
- Number theory and cryptography
- Cryptography and Information theory
- Asymmetric cryptography and key management
- Symmetric Cryptography

UDEMY

- Introduction to Cryptography
- Cryptography with python
- Applied Cryptography with Python
- Complete Cryptography master class

Real Time Applications

- Secure Communication
- Diffie Hellman Algorithm can be used in
  - Transport Layer Security (TLS) / Secure Sockets Layer (SSL)
  - Public Key Infrastructure (PKI)
  - Internet Key Exchange (IKE)
  - Internet Protocol Security (IPSec)

Contents beyond the Syllabus

- ElGamal Digital Signature Algorithm
- Schorr Digital Signature Algorithm
- X.509

Mini Projects Suggestions

1.RSA Encryption and Decryption Implementation:

1. Implement the RSA encryption and decryption algorithms in a programming language of your choice.
2. Test your implementation with various key sizes and messages to encrypt and decrypt.

2.Digital Signature Scheme Implementation:

1. Implement a digital signature scheme such as RSA-based or DSA (Digital Signature Algorithm).
2. Demonstrate the generation of digital signatures, verification of signatures, and message authentication.

3.Key Exchange Protocol Simulation:

1. Simulate the execution of a key exchange protocol like Diffie-Hellman or Elliptic Curve Diffie-Hellman (ECDH).
2. Visualize the exchange of keys between two parties and demonstrate how they can securely establish a shared secret key.

4.Secure Communication Application:

1. Develop a simple secure messaging application using asymmetric cryptography.
2. Allow users to generate key pairs, send encrypted messages, and decrypt received messages.

5.Cryptographic Protocols Analysis:

1. Research and analyze a cryptographic protocol like SSL/TLS or SSH.
2. Create a report detailing how asymmetric cryptography is used in the protocol, its security features, vulnerabilities, and possible improvements.

5. Blockchain and Cryptocurrency:

1. Explore the use of asymmetric cryptography in blockchain technology and cryptocurrencies.
2. Implement a simple blockchain or cryptocurrency system emphasizing the role of public-private key pairs for transactions and wallet management.

6. Side-Channel Attacks Experimentation:

1. Study side-channel attacks on RSA implementations (e.g., timing attacks, power analysis).
2. Implement a simple RSA encryption system and demonstrate vulnerabilities to side-channel attacks.

7.Homomorphic Encryption Demonstration:

1. Research homomorphic encryption schemes such as Paillier or Fully Homomorphic Encryption (FHE).
2. Implement a basic demonstration showing how computations can be performed on encrypted data without decryption.

8. Post-Quantum Cryptography Exploration:

1. Investigate post-quantum cryptographic algorithms designed to resist attacks by quantum computers.
2. Implement and compare the performance of classical and post-quantum cryptographic schemes.

9. Security Analysis of Asymmetric Cryptography in IoT Devices:

1. Study the implementation of asymmetric cryptography in Internet of Things (IoT) devices.
2. Identify security challenges and vulnerabilities, and propose solutions or improvements to enhance security.

ASSESSMENT SCHEDULE

S.NO	Name of the Assessment	Portion	Proposed Date
1	First Internal Assessment	Unit-1 &Unit 2	14.08.2025
2	Second Internal Assessment	Unit-3 &Unit 4	22.09.2025
3	Model Examination	Unit 1-Unit 5	28.10.2025

Thank you

Disclaimer:

This document is confidential and intended solely for the educational purpose of RMK Group of Educational Institutions. If you have received this document through email in error, please notify the system manager. This document contains proprietary information and is intended only to the respective group / learning community as intended. If you are not the addressee you should not disseminate, distribute or copy through e-mail. Please notify the sender immediately by e-mail if you have received this document by mistake and delete this document from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.