**Jaipur Engineering College & Research Centre, Jaipur**
**Department of Computer Science & Engineering**

# Information Security System
# [6CS4-03]
# Notes

**Prepared By:**

**Kanishk Jain**
**Ashish Ameria**

**Assistant Prof., CSE**

## VISION AND MISSION OF INSTITUTE

## VISION

To become renowned centre of outcome based learning and work towards academic, professional, cultural and social enrichments of the lives of individual and communities”

## MISSION

M1. Focus on evaluation of learning outcomes and motivate students to inculcate research aptitude by project based learning.

M2. Identify areas of focus and provide platform to gain knowledge and solutions based on informed perception of Indian, regional and global needs.

M3. Offer opportunities for interaction between academia and industry.

M4. Develop human potential to its fullest extent so that intellectually capable and imaginatively gifted leaders can emerge in a range of professions.

## VISION AND MISSION OF DEPARTMENT

## VISION

To become renowned Centre of excellence in computer science and engineering and make competent engineers & professionals with high ethical values prepared for lifelong learning.

## MISSION

**M1:** To impart outcome based education for emerging technologies in the field of computer science and engineering.

**M2:** To provide opportunities for interaction between academia and industry.

**M3:** To provide platform for lifelong learning by accepting the change in technologies

**M4:** To develop aptitude of fulfilling social responsibilities.

# COURSE OUTCOMES

On completion of the course, students will be able to:

CO1: Identify different security attacks, Mechanism, classical and modern encryption techniques.

CO2: Apply random number generation, AES and S-box theory and Implement public key cryptosystem.

CO3: Evaluate message authentication and digital signatures using hash function and IP security.

CO4: Analyze & Implement Water marking technique and strong password protocol in Information Security System.

## PROGRAM OUTCOMES (PO)

1. **Engineering knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
2. **Problem analysis**: Identify, formulate, research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
3. **Design/development of solutions**: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
4. **Conduct investigations of complex problems**: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
5. **Modern tool usage**: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.
6. **The engineer and society**: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.
7. **Environment and sustainability**: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.
8. **Ethics**: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
9. **Individual and team work**: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
10. **Communication**: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.
11. **Project management and finance**: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
12. **Life-long learning**: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

## Program Educational Objectives (PEO)

1. To provide students with the fundamentals of Engineering Sciences with more emphasis in Computer Science & Engineering by way of analyzing and exploiting Engineering challenge

2. To train students with good scientific and engineering knowledge so as to comprehend, analyze, design, and create novel products and solutions for the real life problems.

3. To inculcate professional and ethical attitude, effective communication skills, teamwork skills, multidisciplinary approach, entrepreneurial thinking and an ability to relate engineering issues with social issues.

4. To provide students with an academic environment aware of excellence, leadership, written ethical codes and guidelines, and the self-motivated life-long learning needed for a successful professional career.

5. To prepare students to excel in Industry and Higher education by Educating Students along with High moral values and Knowledge.

## MAPPING CO-PO

| Cos/POs | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 | PO8 | PO9 | PO10 | PO11 | PO12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CO1** | 3 | 3 | 2 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 3 |
| **CO2** | 3 | 3 | 3 | 3 | 2 | 1 | 1 | 1 | 1 | 2 | 1 | 3 |
| **CO3** | 3 | 3 | 3 | 3 | 2 | 1 | 1 | 2 | 1 | 2 | 1 | 3 |
| **CO4** | 3 | 3 | 3 | 3 | 2 | 2 | 2 | 2 | 1 | 2 | 1 | 3 |

## Program Specific Outcome's (PSO)

PSO1: Ability to interpret and analyze network specific and cyber security issues, automation in real word environment.

PSO2: Ability to Design and Develop Mobile and Web-based applications under realistic constraints.

## Syllabus

| SN | Contents | Hours |
|---|---|---|
| 1 | **Introduction:** Objective, scope and outcome of the course. | 01 |
| 2 | **Introduction to security attacks:** services and mechanism, classical encryption techniques- substitution ciphers and transposition ciphers, cryptanalysis, stream and block ciphers. | 06 |
| 3 | **Modern block ciphers**: Block Cipher structure, Data Encryption standard (DES) with example, strength of DES, Design principles of block cipher, AES with structure, its transformation functions, key expansion, example and implementation.<br><br>Multiple encryption and triple DES, Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback mode, Output Feedback mode, Counter mode. | 06 |
| 4 | **Public Key Cryptosystems with Applications:** Requirements and Cryptanalysis, RSA cryptosystem, Rabin cryptosystem, Elgamal cryptosystem, Elliptic curve cryptosystem. | 06 |
| 5 | **Cryptographic Hash Functions, their applications:** Simple hash functions, its requirements and security, Hash functions based on Cipher Block Chaining, Secure Hash Algorithm (SHA).<br><br>Message Authentication Codes, its requirements and security, MACs based on Hash Functions, Macs based on Block Ciphers. Digital Signature, its properties, requirements and security, various digital signature schemes (Elgamal and Schnorr), NIST digital Signature algorithm. | 05 |
| 6 | **Key management and distribution:** symmetric key distribution using symmetric and asymmetric encryptions, distribution of public keys, X.509 certificates, Public key infrastructure. Remote user authentication with symmetric and asymmetric encryption, Kerberos<br><br>Web Security threats and approaches, SSL architecture and protocol, Transport layer security, HTTPS and SSH. | 04 |
| | **Total** | **28** |

# LECTURE PLAN

**JAIPUR ENGINEERING COLLEGE AND RESEARCH CENTRE**

**DEPARTMENT OF COMPUTER SCIENCE ENGINEERING**

**LECTURE PLAN**

| | |
|---|---|
| **Subject: Information Security System ( 6CS4-03)** | **Year/Sem: III/ VI** |
| **No. of Lecture Reqd./(Avl.) : 30 / 30** | |
| **Semester Starting:** | **Semester Ending:** |

| **Unit No./ Total Lecture Reqd.** | **Topics to be Delivered** | **Lect. Reqd.** | **Lect. No.** |
|---|---|---|---|
| **Unit-1 (1)** | Objective, Scope , Outcome of the course. | 1 | 1 |
| **Unit-2 (6)** | Introduction to security attacks | 1 | 2 |
| | services and mechanisms | 1 | 3 |
| | Classical encryption techniques | 1 | 4 |
| | substitution ciphers and transposition ciphers, | 1 | 5 |
| | crypt analysis | 1 | 6 |
| | Stream and block ciphers | 1 | 7 |
| **Unit 3- (6)** | Modern Block Ciphers: Block ciphers structure | 1 | 8 |
| | Data Encryption Standard(DES), Strength of DES | 1 | 9 |
| | Design principle of block cipher | 1 | 10 |
| | AES with Structure, Key Expansion | 1 | 11 |
| | Multiple Encryption and triple DES | 1 | 12 |
| | Cipher Block Chaining Mode, Cipher feedback mode, Counter mode | 1 | 13 |
| **BC-1** | **IDEA 64 Bit Encryption & MD5 Message Digest Algorithm** | 1 | 14 |
| **Unit 4- (6)** | Public Key Cryptosystems: Requirements | 1 | 15 |
| | Public Key Cryptosystems: Analysis | 1 | 16 |
| | RSA Cryptosystem | 1 | 17 |
| | Rabin Cryptosystem | 1 | 18 |
| | Elgamal Cryptosystem | 1 | 19 |
| | Elliptic Curve Cryptosystem | 1 | 20 |
| **Unit 5- (5)** | Cryptographic Hash Functions, Hash Function based on Cipher Block Chaining | 1 | 21 |
| | Secure Hash Algorithm | 1 | 22 |
| | Message Authentication Code | 1 | 23 |
| | MAC based on Hash Function & Block Cipher | 1 | 24 |
| | Digital Signature, Various Digital Signature Schemes, NIST Digital Signature | 1 | 25 |
| **BC-2** | **IP Security with Strong Password Protocols** | 1 | 26 |
| **Unit 6- (4)** | Key Management & Distribution, X.509 Certificates | 1 | 27 |
| | Remote User Authentication | 1 | 28 |
| | Web Security Threats, SSL Architecture | 1 | 29 |
| | Transport Layer Security, HTTPs & SSH | 1 | 30 |

**References:**

1) Stalling Williams: Cryptography and Network Security: Principles and Practices, 4th Edition, Pearson Education

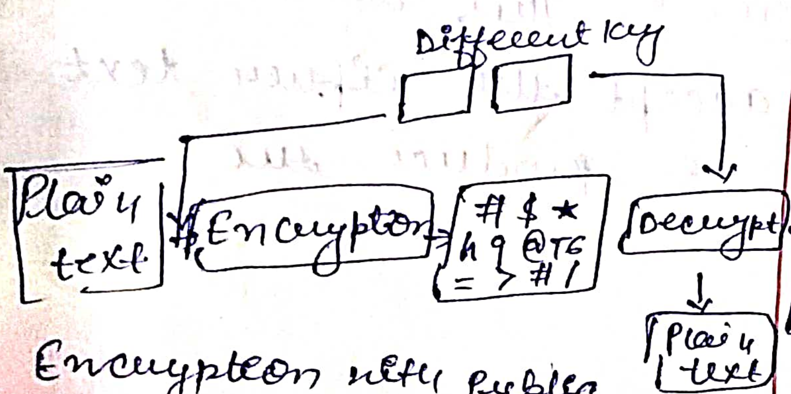
2) Trappe & Washington, Introduction to Cryptography, 2nd Ed. Pearson.

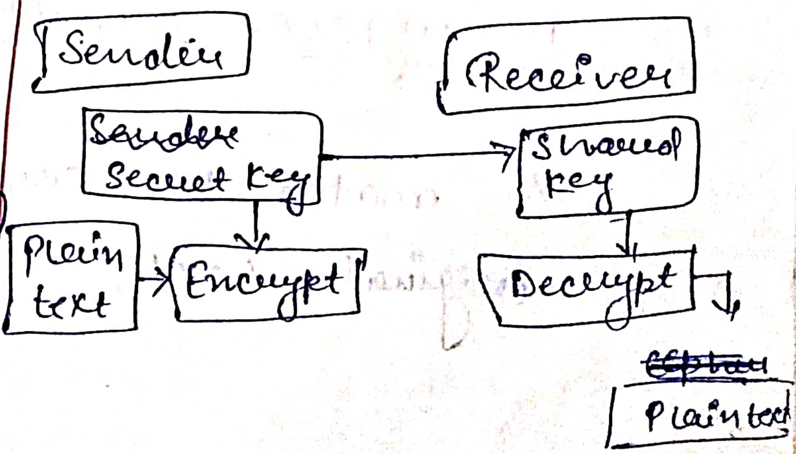
3) Kaufman Charlie et.al; Network Security: Private Communication in a Public World, 2nd Ed., PHI/Pearson

# Unit-3rd

## Symmetric & Asymmetric Key Encryption:-

| Asymmetric Key | Symmetric |
|---|---|
| (i) Different key use | 1) Same key used |
| (ii) Encryption is done with the help of user's Public key & decryption is with help of Private key. | II) Both Encryption & Decryption are done by user's private key / Secret key |
| (iii) C.T. may be of large size | (iii) C.T. same or lesser. |
| (iv) No Problem of key exchange. | (iv) Problem of key Exchange. |
| V) It is used for confidentiality, digital signature. | V) Confidentiality |
| Vi) Process is Slow | Vi) Process is Fast |




Encryption with Public key of Receiver and Decrypt with the Private key

Encryption with the Private key & Decrypt with Public key

## Principle of Public key Cryptosystem :-

1) Plain Text :- This is original or readable message & data that is fed into the algorithm.

2) Encryption Algorithm :- It is the value that is known to the sender. & encryption algorithm performs various transformation on the plaintext.

3) Public & Private key :- This is the pair of key, in this if one is used for Encryption & another is used for Decryption.

4) Cipher Text :- This is the output of plaintext. & depends on the plain text & key.

5) Decryption Algorithm :- This algorithm accept the cipher text & match the key & produce the original text.

## Public key crypto algorithms :-

There are two most used public key algorithm.

1) RSA
2) Diffie Hellman

### 1) The RSA Algorithm :-

→ The system was invented by three scholars Ron Rivest, Adi shamir, Leonard Adleman. hence it is termed as RSA cryptosystem.

→ This is most popular asymmetric key cryptographic algorithm.

→ This algorithm is based on mathematical fact.

**Algorithm :-** 1) Choose Two large prime p, & q.

2) Calculate $n = p * q$ let n be a large no.

3) Select the public key (i.e encryption key) E (p-1).(q-1) not the factor of (p-1)(q-1)

4) Select the private key D :-

$(D \times E) \bmod (p-1) \times (Q-1) = 1$

5) for Encryption, calculate the cipher text from plain text.

$$CT = PT^{E} \bmod N$$

6) Send CT as the cipher text to the receiver.

7) for decryption, calculate the plain Text from cipher text.

$$PT = CT^{D} \bmod N$$

**Example:- 1**

| | |
|---|---|
| 2 | 72 |
| 2 | 36 |
| 2 | 16 |
| 3 | 9 |
| 3 | 3 |
| | 1 |

~~2~~ ~~3~~ 5 ~~7~~ 11 13 ...

1) $p = 7$

$q = 13$

2) $n = p * q$

$n = 7 \times 13 = 91$

$\phi(n) = (P-1) * (Q-1)$

3) $(P-1) = 7-1 = 6$

$(q-1) = 13-1 = 12$

totient function

4) $6 \times 12 = 72 \rightarrow (1 < e < \phi(n))$

$\rightarrow e = 5$

$(D \times 5) \bmod 72 = 1$ $\quad (1 < 5 < 72)$

- e Public key & choose as random

~~$d = \frac{1 + K\phi(n)}{n}$ (k is random no. start with 0 but only use Integer value)~~

~~$d = \frac{1 + \cdot 72}{5}$~~

91

| Row | a | | b | | d | | K | |
|---|---|---|---|---|---|---|---|---|
| 1 | $a_1$ | 1 | $b_1$ | 0 | $d_1$ | 72 | $k_1$ | – |
| 2 | $a_2$ | 0 | $b_2$ | 1 | $d_2$ | 5 | $k_2$ | +14 |
| 3 | $a_3$ | 1 | $b_3$ | −14 | $d_3$ | 2 | | 2 |
| 4 | $a_4$ | −2 | $b_4$ | 29 → | $d_4$ | 1 | | 2 |
| 5 | $a_5$ | 5 | | −72 | | 0 | | ∞ |
| 6 | | | | | | | | |

Euclidean Theorem :-

$\phi x + ey = gcd(\phi, e)$

$(72 \times -2) + 5 \times 29 = gcd(72, 5)$

$-144 + 145 = gcd(72, 5)$

1

$d = 29$

$(d \times e) \bmod \phi(n) = 1$

$29 \times 5 \bmod 72 = 1$

$\frac{29 \times 5}{72} = 1$

$= \frac{145}{72} = 1$

$= 1 = 1$

$a_3 = a_1 - (a_2 \times k_2)$

$a_4 = a_2 - (a_3 \times k_3)$

$b_3 = b_1 - (b_2 \times k_2)$

$d_3 = d_1 - (d_2 \times k_2)$

$k_3 = \frac{d_2}{d_3}$

$k_2 = \frac{d_1}{d_2}$

$d_4 = d_2 - (d_3 \times k_3)$

$1 - (0 \times 14)$

$1 - 0 = 1$ ✓

$0 - (1 \times 14)$

$-14$

$1 - (0 \times 14)$

$1 - 0$

(1)

$a_4 = 0 - ($

$\frac{72}{5}$

$= 14$

5) $CT = PT^E \bmod N$

Let :- Plain text = 10

$CT = 10^5 \bmod 91$

$= 100000 \bmod 91$

$= 82$

$PT = CT^D \bmod N$

$= 82^{29} \bmod 91$

$= 10$

ex. 2

$P = 7$
$Q = 17$

Plain text = 10
$D = 77$
$e = 5$

if d is (−) than:–

(i) $d < \phi$ : $d = d + \phi$

(ii) $d > \phi$

$d = d \bmod \phi$

| Row | | a | | b | d | K |
|---|---|---|---|---|---|---|
| 1 | $a_1$ | 1 | $b_1$ | 0 | 96 | – |
| 2 | $a_2$ | 0 | $b_2$ | 1 | 5 | 19 |
| 3 | $a_3$ | 1 | $b_3$ | −19 | 1 | |
| 4 | | | | | | |
| 5 | | | | | | |
| 6 | | | | | | |

$\frac{d_1}{d_2} = \frac{96}{5} = 19$

1) $P = 7$
$Q = 17$

2) $N = 7 \times 17 = 119$

3) $\phi n = 6 \times 16 = 96$

4) $E = 5$

$(D \times E) \bmod \phi(n) = 1$

$(77 \times 5) \bmod 96 = 1$

$385 \bmod 96 = 1.$

$1 = 1$ (PT = 10)

5) $CT = PT^E \bmod 119$

6) $PT = CT^D \bmod N$ $10^5 \bmod 119$

= 10 Ans.

$a_3 = a_1 - (a_2 \times K_2)$

$1 - 0 \times 19$

$= 1$

$b_3 = 0 - (1 \times 19)$

$= 96 - (5 \times 19)$

$96 \times 4$
384

$d = d + \phi$

$-19 + 96$

$d = 77$

Example :- $n = 11$
$g = 7$

another random no $x = 3$

2) $A = g^x \bmod n$

$A = 7^3 \bmod 11$

$A = 343 \bmod 11 = 2$

3) Alice sends 2 to Bob.

4) $B = g^y \bmod n$ $(y = 6)$

$B = 7^6 \bmod 11$

$= 117649 \bmod 11 = 4$

5) Bob sends 4 to Alice.

6) Now A compute the secret key : K1.

$K_1 = B^x \bmod n$

$K_1 = 4^3 \bmod 11$

$K_1 = 64 \bmod 11$

$= 9$

7) B now computes the secret key $K_2$

$K_2 = A^y \bmod n$

$= 2^6 \bmod 11$

$= 64 \bmod 11$

$K_2 = 9$

## Problem with the algorithm :-

Diffie Hellman key Exchange algorithm can fall prey to the man in middle attack. & is also called bucket bridge attack.

1)

| Alice | Tom | Bob |
| --- | --- | --- |
| → A = 2 | Tom intercepts the value of A sent by Alice to Bob and sends Bob his own A | |
| | → | A = 9 |
| | Tom intercepts the value of B sent by Bob to Alice and sends Alice his own B | ← B = 8 |
| ← B = 4 | | |

2)

| Alice | Tom | Bob |
| --- | --- | --- |
| A = 2 B = 4* | A = 2<br>B = 8 | A = 9*<br>B = 8 |

**Man in Middle attack**

8) Alice | Tom | Bob

$K_1 = B^x \bmod n$

$4^3 \bmod 11$

$64 \bmod 11$

$= 9$

$K_1 = B^z \bmod n$

$= 8^8 \bmod 11$

$= 5$

$K_2 = A^y \bmod n$

$2^6 \bmod 11$

$= 9$

$K_2 \; A^y \bmod n$

$9^9 \bmod 11$

$= 5$

Tom needs two keys. This is because at one side, Tom wants to communicate with alice using a shared symmetric key (9) & on the other hand, he wants to communicate with Bob using a different key (5).

<u>The Security of RSA</u> :- The security of the RSA Cryptosystem is based on

Two mathematical problem :-

The problem of Factoring large no. & the RSA problem.

four possible approaches to attaking the RSA algorithm :-

1) <u>Brute Force</u> :- This involves trying all possible private keys.

2) <u>Mathematical attacks</u> :- These are several approaches, all equivalent in effort to factoring the product of two primes,

3) Timing Attacks :- These depends on the running time of the decryption algorithm.

4) Choosen ciphertext attacks :- This type of attack exploits properties of the RSA algorithm.

1) Key Generation :-

2) Speed

3) Key Distribution

4) Timing Attack

5) Adaptive Choosen Cipher Text Attacks

KEY Management :- It is deal with Secure Generation, distribution and Storage of key Secure method of key management is important.

One of the major role of Public-key Encryption is to address the Problem of key distribution.

1) The distribution of public key

2) Distribution of Secret key using Public key Cryptography

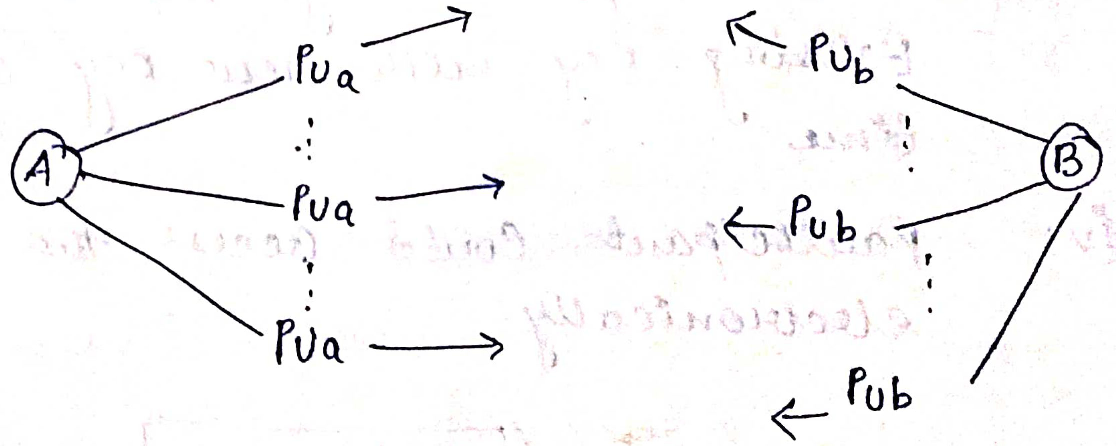
## Distribution of Public key :-

Several Techniques have been proposed for the distribution of public key.

1) Public announcement
2) Public available directory.
3) Public key authority
4) Public key Certificates

### 1) Public announcement of Public key :-

The point of public key encryption is that the public key is public.
If there is some broadly accepted public key algorithm, such as RSA, any one can send his / her public key to any other one or broadcast the key.



**Public available directory** :- A greater degree of security can be achieved by maintaining a public available dynamic directory of public key.

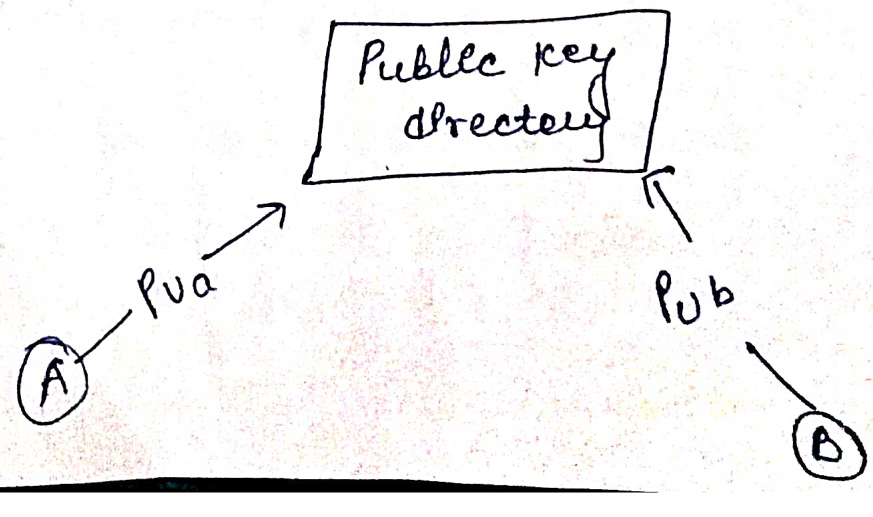
2) Maintainance and distribution of the public directory would have to be the responsibility of some trusted entity or organization.

(i) The authority maintains a directory with a (name, public key) each participants entry on this.

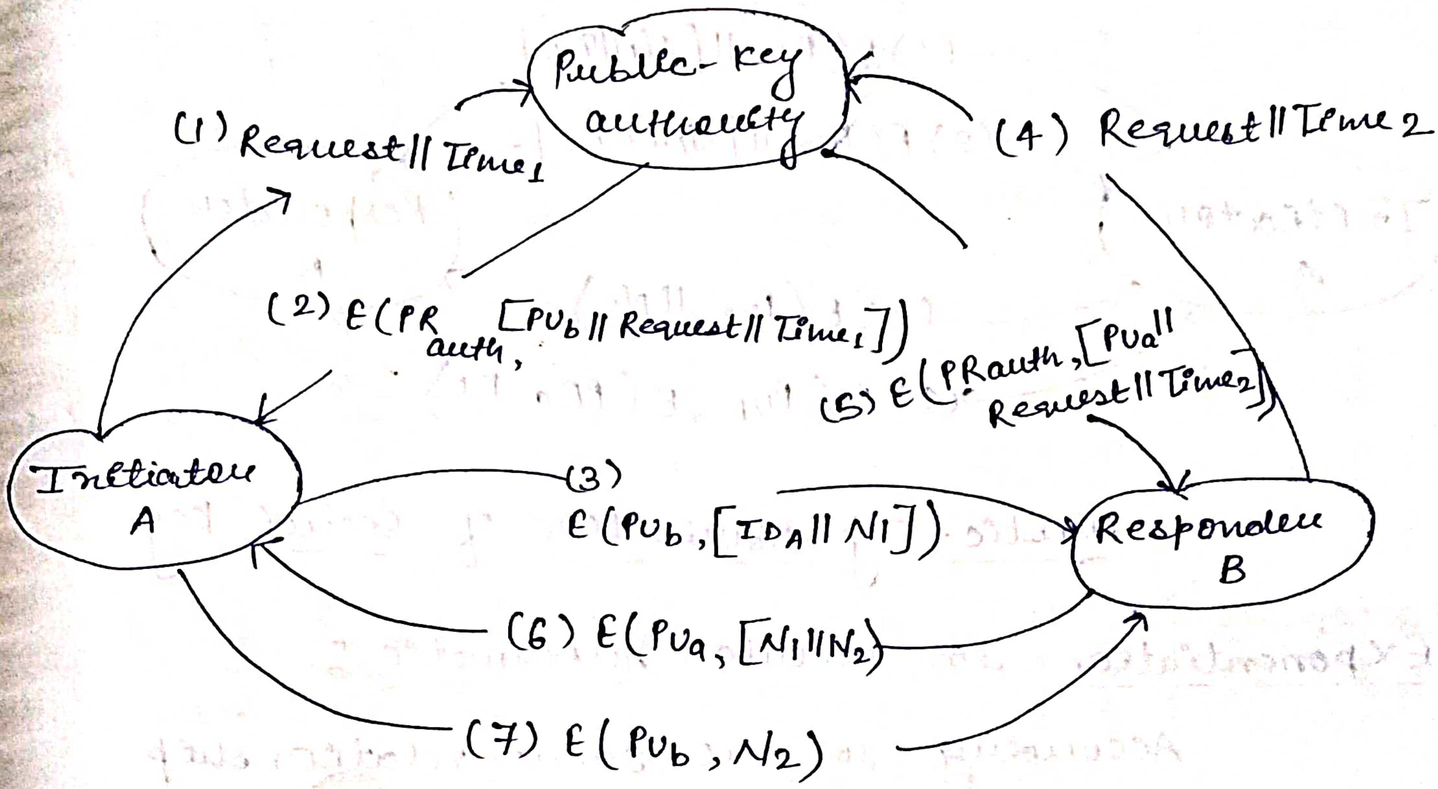
(ii) Each participant register a public key with the directory authority.

(iii) A participant may Replace the Existing key with new key at any time.

(iv) Participant Could access the directory electronically.

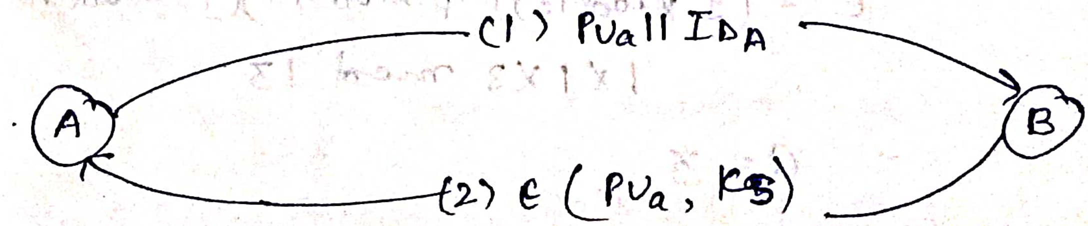


**Public key Authority** :- Security for public key distribution can be achieved by providing tighter control over the distribution of public key from the directory.

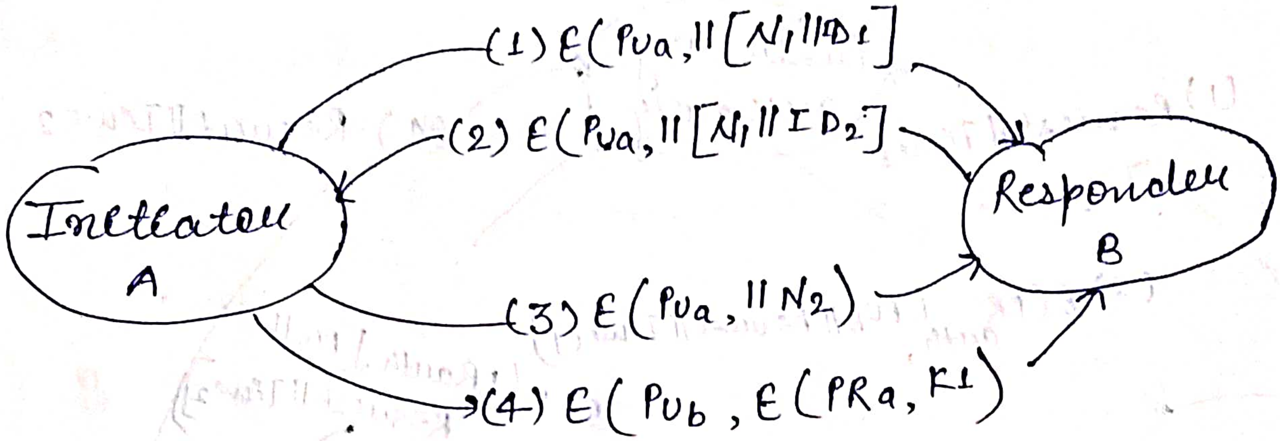



**Distribution of Secret keys Using Public-Key Cryptography**

An extremely simple scheme was put forward by Merkle



## Secret Key Distribution with Confidentiality and Authentication :-




Public-key distribution of secret key

## Exponentiation in Modular Arithmetic :-

According to the same relationship as exponentiation in normal arithmetic. Namely given a modulus n & integer a & b, $a^b$ is defined as that no. C such that

$$C = a^b \bmod n$$

$$C = 9^{11} \bmod 13$$

$$C = (9^3 \bmod 13)(9^3 \bmod 13)(9^2 \bmod 13) \,|\, 13$$

$$1 \times 1 \times 3 \bmod 13$$

$$C = 3$$

# Discrete Logarithms :-

The Power of an Integer, modulo n:

It is natural no. to consider the multiples of a given element a, modulo n, it is often natural to consider the sequence of Power of a, modulo n,

$$a^0, a^1, a^2 \ldots \text{ modulo } n.$$

Indexing from 0, the $0^{th}$ value in this sequence is $a^0 \bmod n = 1$.

Ex. Power of 3 modulo 7 are :-

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| $3^i \bmod 7$ | 1 | 3 | 2 | 6 | 4 | 5 | 1 | 3 | 2 | 6 |

According to euler theorem that, for every a & n that are relatively prime:-

$$a^{\phi(n)} = 1 \pmod n$$

where $\phi(n)$, Euler's function, is the no. of positive integer less than n & relatively prime to n,

$$a^i = 1 \pmod n$$

Ex. Power of 7, modulo 19.

$7^1 \bmod 19 = 7$

$7^2 \bmod 19 = 49 \bmod 19 = 11$

$7^3 \bmod 19 = 343 \bmod 19 = 1$

## Modular Multiplication Using Intermediate Modulo-n Reductions :-

When multiplying no. using modular arithmetic, we can evaluate the expression 911 mod 13.

The basic property that we are going to exploit to do this :-

$$(xy) \bmod n = (x \bmod n)(y \bmod n) / \bmod n$$

Ex. 1) x & y are lesser than n.

$$C = (132)(151) \bmod 13$$
$$= 19932 \bmod 13$$
$$= 3$$

But using the above property we can do this :-

$$C = (132 \bmod 13)(151 \bmod 13) \bmod 13$$
$$= (2)(8) \bmod 13$$
$$= 16 \bmod 13$$
$$= 3$$

## Properties of modular arithmetic :-

The set $Z$, as the set of non-negative integer less than $n$.

$$Z_n = 1, 2, 3, \ldots (n-1)$$

Properties :-

1) Commutative law :- $(V + x) \bmod n = (X + v) \bmod n$
$(V \times x) \bmod n = (X \times v) \bmod n$

2) Associative law :- $[(V+x) + y] \bmod n$ $[v + (x+y) \bmod n]$
$[(V \times x) \times y] \bmod n$ $[V \times (x \times y) \bmod n]$

3) Distributive law :- $(v + (x+y)) \bmod n = (V + x) + (V + y) \bmod n$
$(v + (x \times y)) \bmod n$
$(v + x) * (v + y) \bmod n$

4) Identities :- $(0 + v) \bmod n = V \bmod n$
$(1 + v) \bmod n = v \bmod n$

5) Additive Inverse :- $(-v)$ $V + Z = 0$
for each $V \in Z$

## Operation on Modular Arithmetic :-

The (mod n) operator maps all integer into set of all integers $\{0, 1, 2 \ldots (n-1)\}$

1) $[(a \bmod n) + (b \bmod n)] \bmod n = (a+b) \bmod n$

(2) $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

(3) $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$

**Division :-** Division is essentially the Inverse of multiplication.

Division find the Quotient of two No., the dividend divided by the divisor. Any dividend divided by 0 is undefined.

$$a \div b = a \times \frac{1}{b}$$

**Fermat's Theorem :-**

This theorem state the following :-

If $p$ is prime & $a$ is positive No. not divisible by $p$.

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

$$a^{p-1} \bmod p = 1$$

$$a^{p} \bmod p = a$$

$a^{p} - a$ is divisible by $p$

Another Statement is :-

If $a$ & $p$ are Co-prime.

$a^p - a$ is divisible by $p$

$a(a^{p-1} - 1)$ is divisible by $p$

$(a^{p-1} - 1)$ is divisible by $p$.

Ex. 4, 3 → co-prime

$a = 4$

$p = 3$ (Prime)

$4^{3-1} - 1 \mod 3$

$4^2 - 1 \mod 3$

$16 - 1 \mod 3$

$15 \mod 3$

Ex:-

$28^{28} \mod 13$

$2^{1000} \mod 7$

$24^{42} \mod 9$

$40^{40} \mod 19$

Ex. $3^{201} \mod 11$

$A = 3$

$P = 11$

$3^{11-1} = 1 \mod 11$

$3^{10} = 1$

$(3^{10})^{20} \cdot 3^1 \mod 11$

$(1)^{20} \cdot 3 \mod 11$

$1 \cdot 3 \mod 11$

3 Ans.

[illegible] :-

## X.509 Authentication Services :-

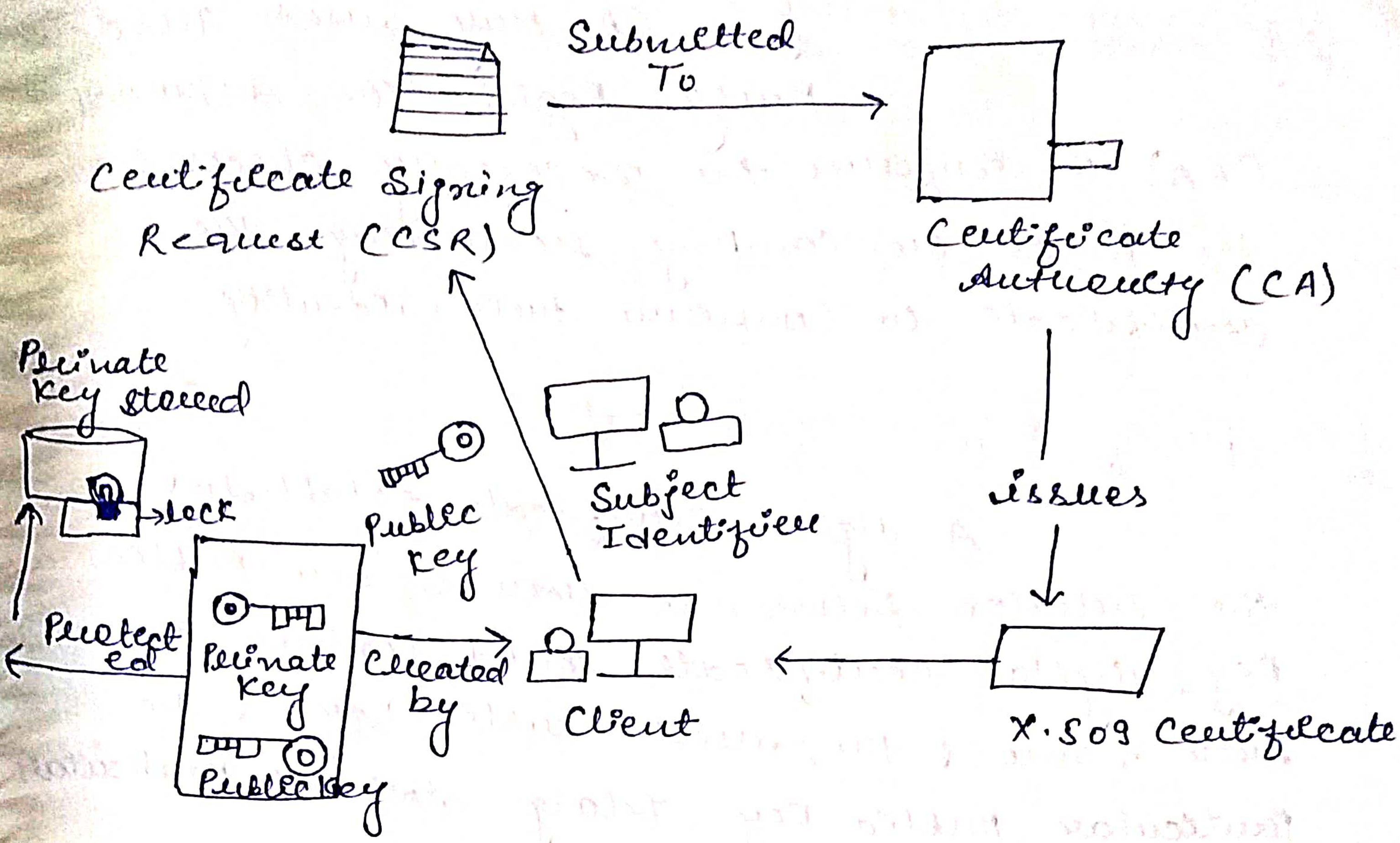
A Standard called as X.509 defines the Structure of a digital certificate.

A certificate can be considered as the ID card issued to the person. People use ID cards such as driver's License, Passport to prove their Identity.

A digital certificate does the Same basic thing in the electronic world, but with one difference.

Digital certificate are not only issued to People but they can be issued to computer, Software Package or anything else that need to prove the Identity in the electronics world.

The Process of obtaining Digital Certificate by a Person / entity is depicted in the following.




CA accept the application from a client to certify his public key. The CA, after verifying identity of client, issue a digital certificate to that client.

Certifying Authority (CA) :- The CA issues the certificate to a client & assists other users to verify the certificate. The CA takes responsibility for identifying correctly the identity of the client asking for a certificate to be issued. & ensure that the information contained within the certificate is correct and digitally signs it.

**Registration Authority :-** CA may used Third-Party Registration Authority (RA) to perform the necessary checks on the person or company requesting the certificate to confirm their identity.

**Example of Digital certificate :-**

A digital certificate establishes the relation between a user & her public key, digital certificate must contain the user name & the user's public key. & The particular public key belongs to the particular users.

Digital certificate

| | | |
|---|---|---|
| Subject Name | : | Atul Kahate |
| Public key | : | <Atul's key> |
| Serial No. | : | 1029101 |
| other data | : | Email |
| Valid from | : | 1 Jan 2007 |
| Valid to | : | 31 Dec 2015 |
| Issuer Name | : | Verisign |

**Technical Details of Digital Certificate :-**

The various fields of a digital certificate according to the X.509 Standard.

It also specifies which version of standard contain which field.

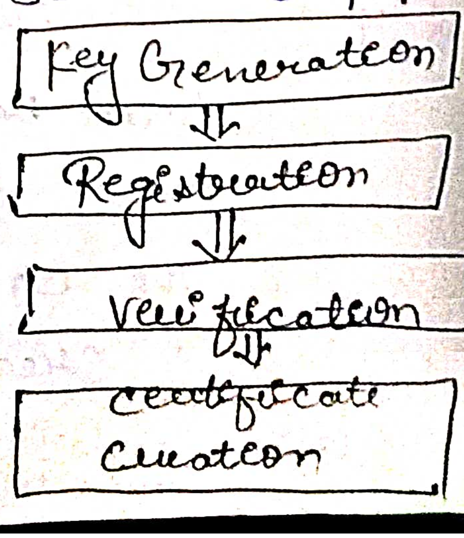
Version 1 of the X.509 standard contains seven basic fields, version 2 added two more fields & version 3 added one more field. These additional fields are called extensions or extended attributes of version 2 & 3.

| Fields | Version |
|---|---|
| Version<br>Certificate Serial No.<br>Signature Algorithm Identifier<br>Issuer Name<br>Validity (Not Before / Not After)<br>Subject Name<br>Subject Public Key Information | Version-1 |
| Issuer unique Identifier<br>Subject Unique Identifier | Version 2 |
| Extensions | Version 3 |
| Certificate Authority Digital Signature | All versions |

<u>Concept of digital certificate</u>

<u>Certificate Creation Steps</u>:- The creation of digital certificate consists of several steps.

1) Key Generation
2) Registration
3) Verification
4) Certificate Creation



Step-1 Key Generation :- the subject (who ...) who wants to obtain a certificate.

1) The subject can create a Private key & Public key pair some software & the subject must keep the private key secret. or public key sends along with other information.

Step-2 Registration :- This step is only for if the user generates the key pair in the first step. & then RA start the process regarding to Registration information (Subject Name, Email ID, country, organization, etc)

Step-3 Verification :- After the registration process is complete, the RA has to verify the user's credentials.

1) RA needs to verify user's details, ~~evidence~~ evidences provided are correct & that they are acceptable if yes that go to Certificate Authority.

Step-4 Certificate Creation :- If all steps have been successful, the RA ~~Request~~ passes on all details ~~...~~ to the CA.

The CA does own verification (if Required) & create the digital certificate.

## Diffie - Hellman Key Exchange Algorithm :-

It is an asymmetric key algorithm used for public key cryptography. This algorithm can be used only for agreement, but not for encryption or decryption of message.

The Diffie Hellman key exchange algorithm is based on mathematical principles, it is very simple to understand.

## Description of the Algorithm :-

Let as assume that Alice & Bob want to agree upon a key to be used for encrypting/decrypting message that would be exchange b/w them.

1) Firstly Alice & Bob agree on two no. prime no. $n$ & $g$. These two integers need not be kept secret.

2) Alice choose another large no. $x$ and calculate A

$$A = g^{x} \bmod n$$

3) Alice sends the no. A to Bob.

4) Bob independentally choose another large random integer $y$ and calculate B $\quad B = g^{y} \bmod n$

5. Bob sends the no. B to Alice.

6. A now computes the ~~same~~ secret key K1

$$K1 = B^x \bmod n$$

7. B now computes the secret key K2

$$K_2 = A^Y \bmod n$$