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. 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). 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 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 - II nd

AES Advance Encryption Standard Algorithm :-

AES comprise three block cipher, AES-128, AES-192, AES-256. Each cipher encrypt and decrypt data in blocks of 128-bit using cryptographic keys of 128, 192, 256 bits. Symmetric en secret key & size use the same key for encrypting en decrypting.

1) We use 128 bit in AES. As compare to DES, AES is more strong.

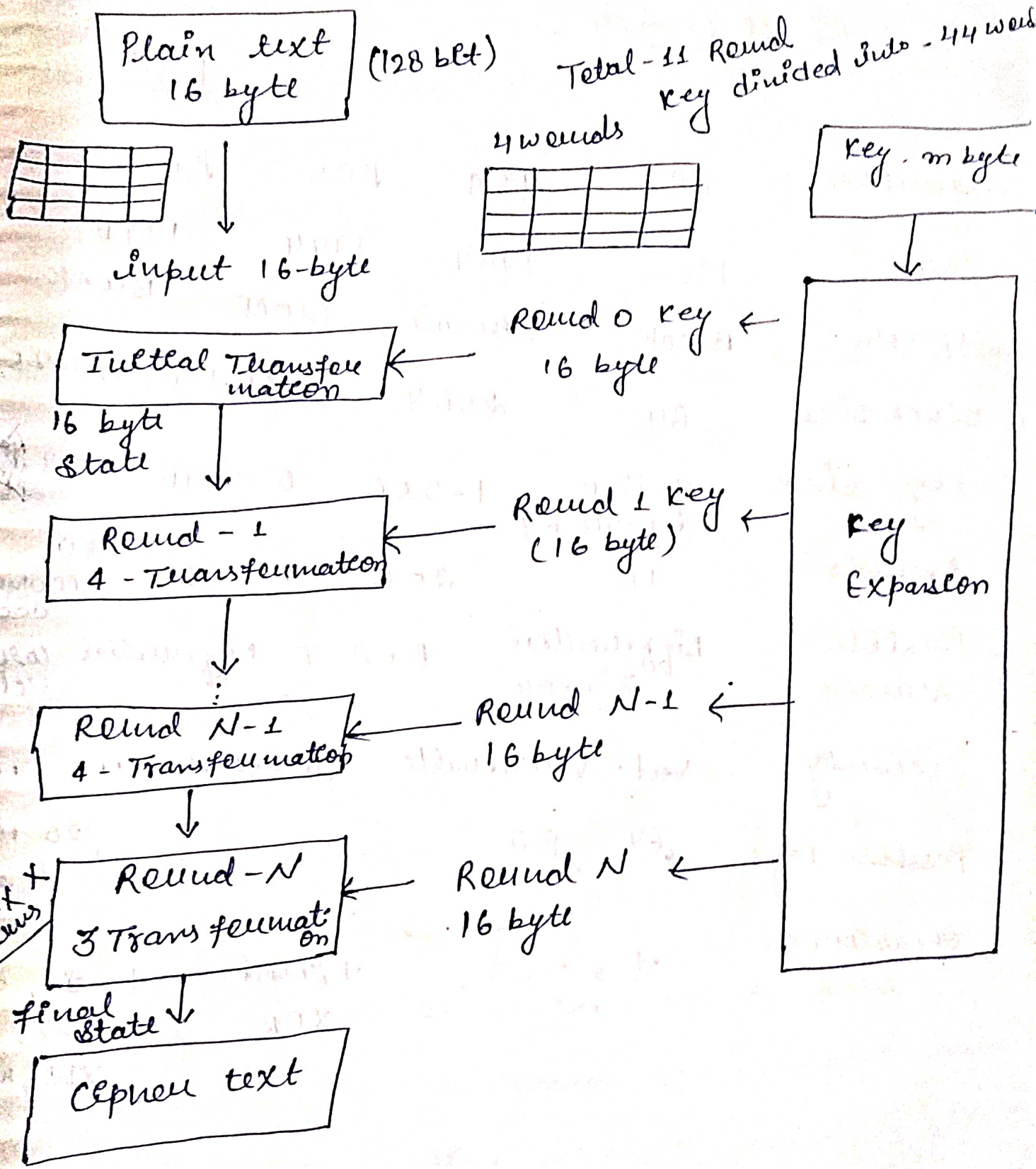
2) No. of Rounds are not fix depend on the key size.

3) if you apply 16 byte key than no. of rounds is 10.

24 byte - 12

32 byte → 14

4) we start the Round from 0 in 16 byte & Rounds go through the 11. 0 round is not considerable. In 0th round we apply the key & then consider the Rounds.



Usual Rounds

1) Substitution
2) Shift Rows
3) Mix Columns

} Particular Rounds process in AES

RC → Rivest Cipher :-

Algorithm	RC2	RC4	RC5	RC6 (AES)
Year	1987	1987	1994	1998
Cipher	Block	Stream	Block	Block
Block size	64	2064	32, 64, 128	128, 256
Key size	8-128 default 64	1-256	0-2048	128, 192, 256
Rounds	16	256	0-255	20 Recommended
Possible Attacks	Differential Linear	BEAST	Differential	Correlation
Security	~~Vat~~ Vulnerable		Vulnerable	" "
Possible keys	2^{64}, 2^{128}	....	....	2^{120}, 192, 256
Operations used	+, -, &, ~		+, mod XOR	+, *, <<<, >>>, XOR, mod

Random Number Generation :-

Random No. are very important to develop the encryption algorithm that are use in security.

Application of Random Number :-

Random value are used for hand shaking to prevent the replay attack.

- RSA Public-key Generation algorithm used for random no.

RNG is a device that is very specifically designed to generate a series of no. or symbol that do not use any specific pattern.

- They appear to auto random.
- Random No. generated by computer are not truly random - over a period of time we can predict them. This is simply because computers are rule based machine which have a finite range for generating random no.

S - Box Theory :- 1) It is Substitution Box & Important component of cryptosystem.

2) It is basic component of symmetric key algorithm.

3) It is based on Confusion & Diffusion.

Confusion :- Is an encryption operation where the relationship b/w key & cipher text is uncertain.

Ex. Substitution.

Diffusion :- Is an encryption operation where the one plain text is spread over many cipher text symbol.

Ex. Bit Permutation.

DES use 8 different S Box, each of contain 64 bit value.

Outer bit 1 & 6.

Inner bit 2 - 5

Result is 8 slots of 4 bits, or 32 bit

S-boxes are boolean mapping $(0,1)^n$, mxn mappings. each component function is a boolean function in n boolean variables.

1) Boolean functions
2) Bent functions
3) Propagation and Nonlinearity
4) Construction of balanced functions
5) S-box design

Boolean functions :- A Boolean function is a mapping from $\{0,1\}$ n $\{0,1\}$.

A Boolean function on n-inputs can be represented in minimal sum (XOR) + of Product (AND) form.

Boolean functions are the building block of Symmetric cryptographic System.

SOP :- Sum of Product

$\bar{A}\bar{B} + \bar{A}B + AB$

$00 + 01 + 11$

POS :- Product of Sum

$(B + \bar{C})(\bar{A} + \bar{B})(\bar{B} + C)$

$0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0$

Bent Function :- It is a special type bent of boolean function.

It takes several input & give one output. each of which have two values 0 & 1. 0 for false, 1 for true.

The simplest example of bent function, written in algebraic normal form are $f(x_1, x_2) = x_1 x_2$ and $G(x_1, x_2, x_3, x_4) = x_1 x_2 + x_3 x_4$. The Pattern continues $x_1 x_2 + x_3 x_4 \cdots + x_{n-1} x_n$ is a bent function. Bent functions exist for even values of n. They are always unbalanced.

Nonlinearity and Propagation :-

The important criteria for cryptography strong boolean function are nonlinearity & Propagation.

upper bound include non linearity.

A boolean function is called the m^{th} order co. relation immune if the o/p distribution does not alter whenever in i/p bits are fixed.

Criteria of S-Box Design :-

1) **Balanced Component Function :-** The component function of the substitution box must be balanced in the manner to ensure a through encryption of of the manage bits.

No Linearity of Component Function High :- High level of non-linearity must be ensured during the design of the component function.

Non-Zero Linear Combination :- Non-Zero Linear combination of component functions must balanced and highly non-linear.

High Algebric Degree :- The component function of S-box must satisfy a high degree of algebric complexity.

Construction of Balanced function :-

Balanced boolean function is a fun" whose output field as many 0's & 1's over its input set This means that for a random input string of bits, the probability of getting 1, is 1/2

Construction :- For n no. of input, the non-linearity of a balanced boolean fun^{n} can't exceed.

$$2^{n-1} - 2^{n/2} + No$$

Here

No. - The maximum achievable non-linearity of a Balanced Boolean function.

For $n=8$ Since the max. achievable non-linearity of balanced function is 4.

For $n=4$, upper bound gives the value of 116

Example :- Let $n=8$ and f be a normal bent function on F_2^8. Without loss of generating Suppose that $f(x,^{0})=0$ $\forall$ $x \in F_2^4$, let h be a bent function on F_2^4. ~~Let to be~~ a $w(h) = 6$ Then by taking any function ρ satisfying the condition in our ~~Conti~~ Construction we have a balanced function g having non-Linearity at least 116.