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.

Cos/POs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
C01	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

MAPPING CO-PO

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	04
	Web Security threats and approaches, SSL architecture and protocol, Transport layer security, HTTPS and SSH.	
	Total	28

	DEPARTMENT OF COMPUTER SCIENCE ENGINEERING LECTURE PLAN		
Subject:	Information Security System (6CS4-03)	Year/Se	em: III/ VI
Just	No. of Lecture Reqd./(Avl.): 30 / 30	1 001/0	
Semester	Starting: Semester Ending:		
Unit			
No./ Total	Topics to be Delivered	Lect.	Lect. No.
Lecture	Topics to be Denvered	Reqd.	Lett. No.
Reqd.			
Unit-1	Objective, Scope, Outcome of the course.	1	1
(1)	Objective, Scope , Outcome of the course.		
	Introduction to security attacks	1	2
	services and mechanisms	1	3
Unit-2	Classical encryption techniques	1	4
(6)	substitution ciphers and transposition ciphers,	1	5
	crypt analysis	1	6
	Stream and block ciphers	1	7
	Modern Block Ciphers: Block ciphers structure	1	8
	Data Encryption Standard(DES), Strength of DES	1	9
Unit 3-	Design principle of block cipher	1	10
(6)	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
	Public Key Cryptosystems: Requirements	1	15
	Public Key Cryptosystems: Analysis	1	16
Unit 4-	RSA Cryptosystem	1	17
(6)	Rabin Cryptosystem	1	18
	Elgamal Cryptosystem	1	19
	Elliptic Curve Cryptosystem	1	20
	Cryptographic Hash Functions, Hash Function based on Cipher Block Chaining	1	21
Unit 5-	Secure Hash Algorithm	1	22
(5)	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
	Key Management & Distribution, X.509 Certificates	1	27
Unit 6- (4)	Remote User Authentication	1	28
	Web Security Threats, SSL Architecture	1	29
	Transport Layer Security, HTTPs & SSH	1	30
Referenc	es:	· · · ·	
) Stalling	g Williams: Cryptography and Network Security: Principles and Practices, 4th Edit	ion, Pears	on Education
	e & Washington, Introduction to Cryptography, 2nd Ed. Pearson. an Charlie et.al; Network Security: Private Communication in a Public World, 2nd		D

LECTURE PLAN

Unet-IV Message Aufhentleateon "- Misg autwillcotton can be flouded using the comptographic techniques that use securt reys as done in case of encoupteon. case of enceripteon. MAC algouettime is à symmetrie reg coupptageaque techniques to periede mig authentecateon: fer establishing MAC Precess, The Sender 4 increance sucre a Symmetric Key K to verify the integerty of message. Receiven B SENDER M Keyk NAC Grenewater SEATOS 4 MAC Grenewater Key K Compare K 1H2 HL Ste3 Step 4 Step 2 Step 1 A 4 B Share a Symmetrice (Secret) key K, ulikeli is net kuneven to augone else. A calculate the MAC by applying key, K to the message M. A then sends the designal message M and 2 MAC HI to B

All Long Solar. When B receives the mag, B also uses K to Calculate les ewon MAC H2 over M. 3. Es Tel CII B nous companies H1 meter H2, if the 2 CII match, B concludes flat the message C-11 My has net been changed during thouset. CH en However, if HI = H2, B sujects the msg, en Mealizing mart the message mar changed en en dueing tuarsult. e Step 3 e Step 2 RE Step 1 e M 1 MAD S M J (MAC) -SENTE E e N ×H2 e 0 HL HL E E **1** ∎ Comparie Step 4 O MIK R R C K (8) (A) e free Message Authentecateon code (MAC) 9 5 Hash Functions - Hash functions are the Ctechniques that is used to C Chiles generates the filigerprent en sumary of C a message that its known as message C. Constant of degest ei hash code of a meg. C C AN PARAMA spectra in program and desist

It is similar to the concepts like geneuæteng the CRC (cyclec Redundancy check of message that is used to verify the integelty of data i.e. to ensure that a message has net been tempened after et leaves the Sender but before it reaches the secciner. Hash function is une valuation of MAC. is hash Function accept a voulable Size message 11 as impet and pereduces a Fixed Size entput known as hash cede. Deigénal data Cold Ingelie May TTT00100 TT011101 00117001 00101001 11100100 enjoinal data ITOTTTO T averiged as siens 00111001 of a list 00101001 OOLOLOOL CRC 5- K 1 1 1 1 1 11100100 TIOTITOT 00TITOOT TOOTOTOOT TOOTOTOOT Origénal data LRC to be senial to kerisron

if the no. of 1's in the column is edd, then we say that the column has odd. Pauly and ilt is indecated by 1, ethermise if the No. of 1'm in the column is even ilt is indecated by 0 in the LRC calcutton process. C

Call

4

C II

er

CO

en

e

en

e

e

e

e

C

e II

e

4

Company

Cincl

Curk

C

Gran

HMAC > Hash based Message Authentleaten code: HMAC has been choosen as a mondatony Securety implementation fou the Internet Prebocol (IP) Securety and is also insed in Secure Socket rayer (SSL) Protocol, is used on the Internet. This HMAC is do reuse the

Existing message digest algouethin, such as MDS OU SHA-L.

Fristing mig digest algerettun Such as MDS ere SHA-1 Ouiginal ricesage Nessage Digest Encempt 7[NAC] ND T Key K d Final cutput MMAC Concept

Message Digest Algeneture :-This concept is Simelon to nosh Finder. Message digest also the fingenperent of the given message. we take the elegend msg block of the message, Vaulable length. Then we use the message digest Algenetium (MDS, SHA) to publice the Fixed F Small Size message digest. alliginal Message (Vallable length) Augenerun Nos] the set of the Message Digest Message Digest Ageelting Here we use the concept that Example : 7391743 multiply each deglet in the no. meter the mext diglet (excuede 0) & dis caudeug une fleust diglt of the multiplication openation,

mo. is 7331743 Deeigenal Result Operation Nucleoply 7 by 3 21 Discard Flust diglt 1 nucltiply 1 by 9 9 nueteply g by g nuclepty 9 by 7 63 Discard flust digle 3 nucleply 3 by 7 12 2 Discould Fleist diglt nultepty 2 by 3 So, final message diget is 6 Message digest colculation puocess MD5 Message Digest algentium Mbs is mig digest algeelettine that mas Imperored developed by Ron Rivest. Mbs is a and the latest verston, The enginal message digest algoulture mos called as MDL. MDS is a fast algeneture that produce 128 bet long mig degest. It take the surpert block S12 bets às cupiet & peroduce the 128 bet block of msg digest as output.

1

G LEI

CEL

1

COL

C-D

C

en

er

CI

C

e

4

c

Wouking Of MAS :- The weaking of the MAS msg digest algenetum can be Classified into the following step.

Step 1 fadding -The Flust step of the MDS is to add padding bilts to the original message. The secason behind this paddling is that we mant to make the length of the Derginal message equal to the values, that is 64 bilt less than the Exact multiple of S12 bits This 64 bets less value new be used Fer length Padding.

Example :- Ty the length of enginal message is 1200 bets, then the we add the Paddeng of 272 bets to make the msg 1472 bet long. Eta was Exact mutteple of S12. (1S36 = S13X3)

Overgenal message A Paddeng bets (1-S12bet New Niessage 64 blits less than the multiple

Step: 2 Append du Longth Field :we calculate due length of the congluate merrage lie. Excluding due Padaling hells). This longth its added at CO the dast aplear due padding bers in -6 due cuigtual message C [] The length of perginal msg CD C is Expressed is the Gubels value. CO e CO meg Paddeng & Length CD C J -> 64 beis -> E- GU ble loss duam C nulleple of S12 bel. 9 C Final mag that well be used for hasking ---> mulleple of S12 bets ----> tep 3 :- Drucde the Input Final Mcg Buto S12 bets Block :-The mag prioduced in the last steep is Craw C dindded into the blocks of S12 bits each. cl c final msg use for hasting cl Blocks Block2 BLOCK3 BLOCK4 -BLOCKM Creat SIZBERS SIZBERS SIZBERS SIZBER C STR.

The last

Pro-

I

Step 4 :- Inttalize Chainling Vaniable :- 1
we take the 4 vaulables known as
Cheenling vandables. They are identified Cheenling vandables. They are identified
Cheeneng Valender of ituese is a 32 bit
as A, B, C & D. Each of ituese is a 32 bit
Manuber. The Hexade comal values of these
cheining Valetable.
326it A OL 23 45 67 twe statts from 0-9 in the pairs, then A-f in the pairs.
DO CO Et Afree filling till Fe-
BA 98 in pairs.
32 10 A=020123950F
3261 D 76 54 02 BEORDED CEA90 D=0276543210
Step S - Purcess Blocks + This is the mein
Step of the affer
The would be the set of the
classified into the Fuertuen Sub-steps.
Step S.1 Copy the 4 chaining valuable into 4
couvesponding valiable a, b, C, d.
Celectesponon
a=A A B C $Db=B$ f f f f
d = D a b c d
Capying mainling vaniables into temporeary vaniable
touchengery variable

R. AN

and the

1/1 Step 52 :- Dérilde the current S12 bits 1 black into 16 sub-blacks of 32 blts 1 4 the product of the each. Cal 6 Block L (SI2 bets) Con 1. 10 1 (Lat. 1. Contra Subblock 1) Subblock 2) -- Bubblock 16 Crat -> 32bets -> > 32 blts -> -> 32 blts -> Contract Currow Sub blocks with in a block Com Step 5.3 :-C we have 4 securds in each sound Carro we precess all the 16 Sub blocks. C The input to the each beaud use C the there thing. C (i) au due 16 bets Sub-blocks. C C (ii) The vallable G, b, C& d. Casto ເທັ່ງ Some constants known as t. C 12 1113 11-11 Carl C C 16 Sub block Constants (it) C THE TOTAL C__ One-Rend Ministering C___ **1**. C__ A Ь C. T da st C Contan an 6 Conceptual pueces metti in C a Reusal aller all tan is a presenting its C C A Para have the interest C

C

C

C-4

d C Q Ь Step (2) P Percess P step (ii) Add K | Step (iii) M[u] > Add Add Step (iv) t[K] Shift Step (V) 2 Step(vi) Add d C 6 a One MOS Operation can north emotically express a single MDS we a = b+ (a+ perocess p(b,c,d)+ M[u]+t[ic]< openation :-1. 115 CIA wheele a, b, c, d' -> chaining vaceables. Perocess P -> A non- Lineau operation M[u'] > it 32 bet wend, Sub block t [K] > a average of constant Cenculore leget surf by 5 bets. 222

1 The Perocess P. 3- The process p is nothing but est. 61 Sonce basec operations on a,b, C, 6 d' The Percess P is défeuent Co C fere all 4 Remd. The percessing of P C Perocess in each Rend. C C Pecocess P Rend F(bicd) = (bnc) V(bind (6 AND C) OR (NOT 6) AND (d) C L G(bierd)=(bnd)v(cnd) (b'AND d) OR (CAND (NOT. 4)) H (bigd) = 60 cOd 2 I(b,c,d) = CO(bvd)BLORC LORd. 3 4 CXOR (bOR (NOT d)) Process of Prin each Rend The strength of MDS o- Whostome stan The attempt of Rivest mas to add as much of complety & handomness as possible to the MOS algenthim, so that no two msg digests publiced by MDS On any two different message are equal. planting and 121 is Large In Trinsance A with the first plate manually

Mash store is also a one way hash function algorithm used: to create digital Signatures. to cucate digteal Signatures. SHA-1 is Sinclose to the MDS algorithms developed by Ron-Rivest - SHA-1 is Slighty slowed than MD5, but it is found to be mene secure, SHA wences mette any imput msg that is less than 264 bets in length. The output of SHA is a mig digest, muller is 160 bets in length (32 bets neace than the may digest publiced by MDS) Wenking of SHA-1 o- LERE MDS, the Flust step 1) Padding in SHA-1 is to add Paddling to the end of the eniginal message. The padding blt always needed, even ist the dougth of the mag alucely nulteple of \$12 bets.

Ouigénal misg (Paddeug betts) (1-(512 bets)

> New nuessage 64 bet dess than the multeple Of S12 bets

Step 2: - APPend length? - The length of the mig Excluding the length of the Padding is now calculated and appended to the end of the Padding os 64 bet - blacks

() Length ougenal Paddling mig IL -> 64 bels -> GU bels less than multiple -> of SI2 bets final may that never be used for nulteple of S12 bets -> strate at as the Input cuto S12 bles blocks "-Step-3;-Dinede The imput message de new, dévided into blecks, each of eight S12 blts. final message use you washing BLOCKN Block2 BLOCKI SI2 blts SIZ bets SIZ bets Instalize 160-bets chevneng vancable ; flve The 160-bet buffer consists of 32-bets register (1, B, C, D, E). Befere processing any block, these sugester are instealized Fellouling Hex Values to the 45 GT 01 23. AB 89 EF CD a fall white all B 98 BA FE. C DC 10 D 32 54 76

T

TEL.

CIL

C

e

C

e

C

C

C

C

C

C

C

C

C....

Catel

C...

G

C

C

C

C

0

the net sets from

Septementers to

the anise between and the

D2

EL

FO

C3

1. In 1 112 AS WINDOW A

Step-S: - <u>Perocess</u> <u>Bleck</u>: -Now actual aggentium begin. Here also, the steps are and Simelaw to those copy of chaining variable - A-E into value jn MDS. Variable a-e. The combination of a-e, called as abcde men be considered as a single register (i) for slowing the temperary final resent. New dividing the current S12 bels block into (11) 16 sub-blocks, each consisting of 32 bits. SHA has Feller Remole, each scends has 20 (11) Steps. each riemols takes the current S12 bets block, the suggister abcde and a constant r(t) (where t=0 to 79).

K(t) un Kennds value of t nexadecimel blw SA 92 79 99 9 L 0 to 19 GE DS EB AL 2 20 to 39 JF IB BC DC 40 to 59 3 CA 62 C1 D6 60 to 79 41 4 rounds are used in SHA. 20 they

ilteration in each nounds, so the total 80 ilteration in SHA.

The logecal operation of SHA:-

(12)

1 intor e d a Ь С fuece 35 p Add Add A [Add K-w[t] 1.131. KEt7 Add F 13 10 e C. alb d can nuette the Mathematically we Atecation perocess :abcde = (e+ perocess P+ S(a) + wCtJ + K(t)) abcde = The register to stone, the Antennealeate and Final values. Puccess P = The logical operation S⁵ = Clerculari left Swigt of the 32 blt Sub-blocks by t blts w(t) = A 32 bles value

UL

Carl Sink

en

C

C

C

C

C

C

C

C

Coal

K(+) = one of the spine additione Constants

The process P : The Percess P of SHA algorithm nas défiguent complex mathematical fouche In each 4- decends. Perocess P Reurol (BANDC) OR (NOT 6) AND (d)) bxorc &ord 1211 (BANDC) OR (BAND d) OR (CANDd) b XOR c XORd 2 not trees Security of SHA-1: - SHA-1 is the most secure message digest algenthing There nome been no successful attacks repontes against the SHA. Because let use Bo étéréations and puoduces 160-bets message digest. Companison between MDS and SHA-1 :-MDS Companison SHA less Secure than Higher Secure SHA. Than MOS. Securety Mgg digest lougth 160 bets 11. 128 bets lot ouginal message 2¹²⁸ openations 2¹⁶⁰ openation 2⁶⁴ Operation sani 2⁸⁰ Operations to break to break message digest Speed Only 80 atenation only 64 Ateration in uses personal in the

Digttal Signature :-VII. Permetives of message authentleateon. CEL CIL CIL It is a techniques that binds a en Peuson/entety to the digetal data. This en binding can be independently verified by e II reciever as well as any triend party. Digetal Signature is a compto guaphile value friert is calculated form the docta. Digetal Signaiture Blandaers makes use of SHA-1 algentium fer calculating the msg digest over an ereginal message & uses the message dégest to perjeun the déglial signature. DSS makes use of an algenething, called as Digital Bignature Argenethur. Dss is standard A DSA is actual agreecture. KSA 4 Digetal Signatures i- we have mentioned Penjeuneng digetal & segnature. used feel Let us understand now alles weaks in Ofter by step fasheon. SENDER (A) wante to sende a msg (M) to receiver (B) along nilter the degetal Signature (5) Calculocled over message (M)

en

e

e

e

e

e

e

C

C

C

C

Child

C

C

CN

Cal

Carlo

The CEMPTON (M) Meser the SHA-1 mig Step 1, 8digest algouistime de calculate the missage algest (MDI) over the Disginal message (N). Deisgimal mig Herage Digert Argonstum SHA-L No start of L B. Miller Digest Message digest calculation The cender (A) new encrypts the Step 2 :mig digest nelte her peinate key The output of this process is called Digltal Bignature (DS) MD1 Encurption DS Sender's Permate rey Neue Sendeu's (A) Sends the Outginal msg(m) along north DS to the recence (B)

Receiven E Alelinour? Sender 10.N 0.M D.S DS

15

CEL

CII

C-11

CII

e D

en

e ji

ep

CE

e

CI

e

e

C

Career

Constant

Contra

C

C

C

C

Com

C

Step 4 :- Ayten une succiven (B) succives the oniginal mig (M) & senden's (M) digetal Bignature, B uses the same message digest algorithm as was used by A & calculate be own mig Negest (MD2). O.M Mig Digest

Algeeretum H Algeeretum HD 9 SHA-2 MD 2

Step-5° - The receiver (B) nous reser the Sender (A's) Public Key to decenypt the degleal signature. A had resed here Perivale Key to Enceypt the O.M. 4 of also use the A's public

to decuypt the message. Jery B new compares the felceneng Step 6 2 message dégests:-MD2, millen is calculated in step 4 MDL, much is returned from A's degetal Bignature In step 5. DS MDI Deccupt metter senders N Public Key MD1 = MD2accept the engenal message (M) is the connect, unaltered message as f.c.om A. is also reject the mag, if mag aus net Same, altered MD1 MD2 ND22 NO Yes accept & Trust Reject the the D.M. Journey (1) plalal Signature verification

0

0

V

3

3

0

3

0

3

0

3

3

9

9

9

)

9

C.C.A 1 Authentecation pustecel :-In flu's puetocel we trying C L CE to autrentecateon of each etness. Beth CII tu pautres au lise authentecation pou CI 0 the secree communication. There are two bread level somewes c II c II for countrying out the outlened. en C -> One way authentecation CTH -> rutual authent cateon C (i) One way authentecateon o-CO C The close behend one-way C authentication is simple. if there are C ture researce A & B. Bautreit cates A, C C but A does net autuent' cate B. we call C II et one-way authent cateon. These and vancous 9 ¢ I ways in niliech type of authentecateon Scheme can be Implemented. 5 One way authentecoteon C Legin Shaved Secret One-way public C C CI Legin Only "-(1) Usen A Sends her resser Cal Carlinge name 4 Passwould in the place text facon to the ether usen B.

Te

B veu fier the reser name and passwend. 2) if the reser name 4 passwend au courect, commund cation starts between AfB, (1) Usermanne A Passward 123 testing B Veurvied Successfully 2 hogen only authentecation Showed Securet ?- There is an assumption that A & B have agreed on a shared Symmetric Key KAB. A sends ner user name and passwerd to B 2. B creates a random livellenge R and Sends it to A. 3. A enceupt the elandom enallenge (R) mette the snalld symmetric key blue Af B (KAB) and sends the encerypted R to B. B also encergets fue eneginal Mandom cuallenge (R) metter fue same Shered Symmetriec Key (KAB). if this encuypted challenge matches mette the one

Sent by A, B Consideer A to be auturite

NURTHA PARA

Usermanne: A B Random Challenge Random Challenge encemptool men ph

Shauled Securit

Carlos

1

1

-

C

C

C

C

en

e

C

C

C

e

C

C

C

C

C

Call

C

C

C

C. Hay

One way public keye -

D' A Sends here desce name to B

2) B Sende the leardon challenge (R) to A. 3) A encaypt the seandon challenge (R) with here prévale key 4 send it to B.

Breser the Public Key of A to decempt the encempted handom challenge, motels melter the oneginal Random Challenge (R).

Usen Mame: A Random Challenge B Randon challenge (R) encuypted to the net A's permaterpy.

One way Rubble Key - Approach - 1

A seuds her user name B.

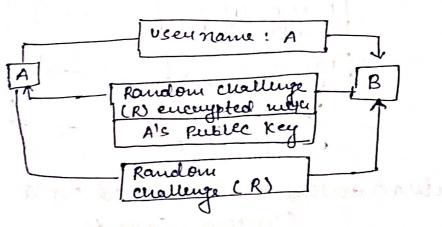
1>

2)

3)

B Creater the scandom challenge (R) and encergets its melter the Public Key of A, B Sends this encergeted scandom challenge to A.

A decouppted the encouppted random challenge (R) with the premate key 4 Send it to B. B matches it wette the oreginal Random Challenge (R)



Mutual Authentication: In this beth of & B beth authentecate

each ether. [Mutual Authentication] [Shared Shared Rublec Keys [Based] Based

1) Sharred Second &- This protocol assennes that A 4 B have a shared Symmetrice key FAB.

> 1) A Sends her user name to B. 2) & sends a soundom challenge RI to A.

A encuypts R1 with KAB and sends it 3.) to B.

A sends à déffecent sandon challerge R2 to B. 4)

A Bar

T

SEL

-

CIE

CE

ear

e

e

CO

CU

C

C

C

C

C,

C.

C

c

cel

Caster

C

C

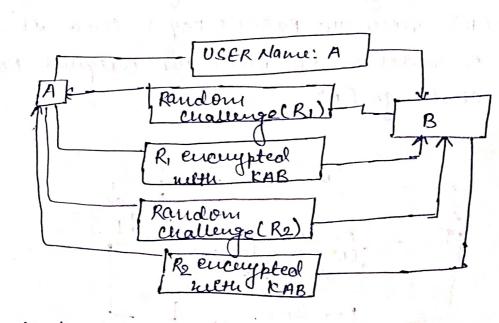
Cher

C.

C

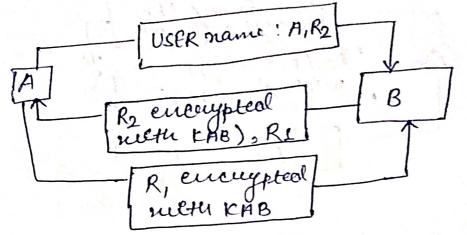
R

B encuepte R2 with KAB & Sends ilt to A. S)



Mutual authentecation based on a Straveral Secret

A sends the user name and a random 1> Challenge (R2) to B. 2) B encupts R2 with the shared Symmetric key KAB, geneuated a neue leardon challenge (Ri) and send these two to A. A vereifier R2, enceupts R1 mith the showed symmetric key LAB, & Send et to &. B venigier RL.



Optimized mutual authentecation based on a suared securet Arrivall

uble keyr: - if de B know each etweis public key, twee message and requered to complete the methal authent-conteon process.

A Sends here sisce name 4 soundom Challenge (R2) energypted with B'S Public Key. B decrypts the seardom enallinge (R2) with his prénate Key. B Creates a new standom challenge (R1) and encerypt it welter A'S public Keys. B Send kno theng (decerypted R2 & encerypted R1) to A. A decrypt the standom challenge (R1) with here perhate Key and Send Stis to B.

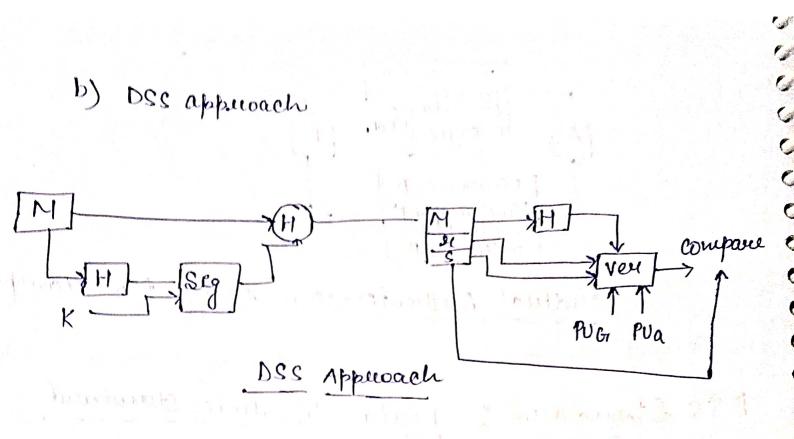
Breufier, Rrisson

1.

12 12 Useermanne A CR2 energlij bier 1 8's STE 1.11 The SRO, (R, cuceupt B) nicth A'c publicity -RI RI c II CI CI A sends her rescre name and R2 to B. B encergpt R2 metter his prevnale key f 1) c III e 2.) CI Send ill & RI to A. A Signs R, and sections it back to A. e e 3 C Useunance: A, R2 C C (A) R2 encuypted (B) (CH4 FAB), R, (B) C C - R, Signed neltu A's perenate Key C C C I Time Stamp - we can reduce the mutual authentication percess to fust C C C two Steps by using timestamps. 1) A Sends here reserve name 4 cuovent Cale truestamp encupted with a Shaced C Symmetric Key (KAB) to B. C C B returnes the concestance by decerpting C I 2.) using KNB and One to the timestamp. C. C l B enoughts the result wetter KBA (net KABI) and send set to A, along wetter here user name. Comment

USer Marine: A truestamp cuesppted the B Uccertance: B (timestamp + 1) encrypted methi KAB rudual Authentecation using tomestamps DSS Standand :- Diglial Signature standand DSS makes use of the Secure Hash algerething & pusents new degleal signature techniques, the deglad Begnative sugerettim. The DSS Apperoach :- The DSS uses an algorething that is designed to puriede Only the degled Signature function. RSA Appuach is use fer tuis signature Standrovel. et is a Public-key techniquer. Compane HH E(PRa, HENJ)

a) RSA approach



A printer and a print of all to come the objection in the second of a second o

and at the state in teally in provident to provide the

antening and any and any princetona.

I DEA? - International Data Encryption Algoliethur "-IDEA is a symmetrie black ceptier digenetium. It was meant to be a suplacement four the Data Encuyption Standaual. Hure plain text in 64 bet. Key is of 128 bet. And it is divided 2> in 52 Sub Keys. Cephen dext is same as the place text 3) that is 64 bet. Number of Adentecal neurols are 8 4> where in each hourd 6 key are used Leke ders 48 keys in dast neurol 5> another 4 Keys (6×8 = 48+4 = 52 total) are being used in beth the Encuyption and decemption feecles. whech d'éférent operations au used. 6) → XOR -> Addeteon -> Mulleptecation

	•
	1
-> The 128 bet key is diveded into 8	4
Sub Paults that is 16 bets each.	
-> K, to KS2 Keys aue generated.	5
Sequence of openation in one Remol :-	0000
1> rulteply PL and K1	e
2) Add P2 and second K2	0
3) Add B3 and thend K3	e
4) rulteply P4 and K4	e
이 것 같은 것 같	5
5) Step D & Step 3	c
6) Step 2 7 Step 4	
7) rulteply step 3 meth FS.	6
a) and nesult of step 6 and step 7.	
uchter marget of Step 8 welter KG	
(0) Add mesult of Step 7 and Step 3	
11) XOR result of Steps 1 and Step 9	
(1) XOR result of Steps 3 and Steps 9.	
13) XOR quart of Steps 2 and Step 10.	
in Jok jusuit of steps I and step It.	- Alton and

Same	operations are perferenced in B rounds-
ĿŻ	rullepty P1 were K43
2)	Aidd P2 and \$50
3)	Add Bs and ESI
4)	ruttepty P4 and FS2.

Tuput place Text (64 bets) PI (16beu) <u>P2 (16bels)</u> P3 (16bels) Py (16bels) Round KI 1 Rend 1 KG e K7 Rend 2 : K12 - K43 Rend 8 1 K48 - 14-9 cutput Tecansfee mateon -k- KS2 →C4(16bets) CI (16 bets) C2 (166els) C3 (16bets) Certput Cephere Text. Bucad und Steps in IDEA

Steps outteply PI and KI Step 2: Add P2 and K2 Step 3 Add P3 and K3 Step 4 : nulteply Py and Kg Step. S XOR the seesuet of step 1 and steps Step 6 XOR the results of Step 2 & step 4 Step7 multiply the result of step 5 with ES the result of Step 8 Add Step 6 & Step 7 Step 9 reultiply the results of Step & welter KG Step 10 Add the susue of Step 7 and step 9 XOR the result of Step11 Step 1 and step 9 Sup 12: XOR the resents of Step 3 and Hep 9

d. int C L COL CIL CI CIL CI en CIE e CI "CTI C CIII C C c c C C Caso C C C C C 5 C

Step 13! XOR the result of step 2 and step 10 Step 14: -XOR the lesult of step 4 Detail of one secural in IDEA Sub-key Grenewatton feu a Remol :-Flust Remol :- The inclear key consists of 128 bets, felone millech 6 sub keys KI and KG are generated for the fourt Rend. Since Ke and KG consists of 16 bets lach, let of the decenal 128 bits, the Flust 96 bets are used for the Flust Rend. P2 Py PL P3 - rulteply Add -Kz k1 Add Nulteply Kg K2 XOR XOR ruelteply KS Add KG rutteply XOR XOR Add XOR XOK FR2 Ra

1.50 Oleganal Key (128 bles) A DE 1 Unused 8215 (97-122) KI (BER 1-16) [12(BER 17-32) --- | 10(BER. BI-36) GO Sub-Key generation for sound 1 5 c 9 Output Terares formation :er The cutput Tuansmattion is en One time openation. It takes place at the C end of the 8th Round. 64 bet value C Cont directed into 4 sub-blacks (say R, to Rg. C each consisting of 16 bets). Your Sub-Keys C Com are applied here and net SPX. Cer

C

C

C

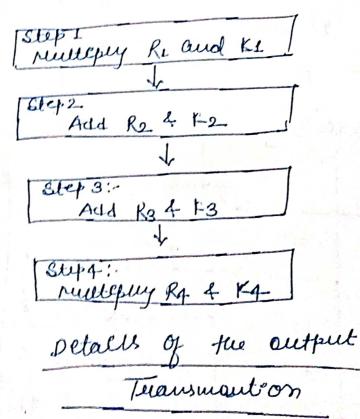
C.

C

C

C

C



cutput of two process is the Fiend 64-The cephere text. which is the combination of ble Feur cephen text sub-blocks. the R.A. K3 RL R2 rultepy / Add F1 > Add K, rultepuy Kra VC4 C3 C2 CL appen Text (entput 64 bets) autput Transfermation Puccess IDEA Decuption :- The decuption puecess is Exactly the same as the encergpteon process. There are some alterateon in the generateon and Pattern of Sub-Keys. The decouption sub-tags are actually inverse of the encuyption sub-Feys. The storength of IDEA :- IDEA uses a 128-bet Key, where is double than the Key Size DES. To Break Suts IDEA 2128 enceryption would be requered.