B.TECH/CSE/7TH SEM/CSEN 4162/2020

CRYPTOGRAPHY AND NETWORK SECURITY (CSEN 4162)

Time Allotted : 3 hrs **Full Marks : 70**

Figures out of the right margin indicate full marks.

Candidates are required to answer Group A and any 5 (five) from Group B to E, taking at least one from each group.

Candidates are required to give answer in their own words as far as practicable.

Group – A
(Multiple Choice Type Questions)

1. Choose the correct alternative for the following: **10 × 1 = 10**

(i) DES works by using
(a) Permutation and Substitution on 64 bit blocks of plain text
(b) Only permutations on blocks of 128 bits
(c) Exclusive ORing key bits with 64 bit blocks
(d) Permutation and Substitution on 64 bit blocks of plain text.

(ii) How can we avoid man-in-the-middle attack?
(a) Accept every SSL certificate, even the broken ones
(b) Use connections without SSL
(c) Use HTTPS connections and verify the SSL certificate
(d) None of the above.

(iii) The _________ cipher reorders the plain text to generate the cipher text.
(a) Substitution (b) Transposition
(c) Both (a) and (b) (d) None of the above.

(iv) ECB and CBC are —
(a) Block Cipher (b) Stream Cipher
(c) Both (a) and (b) (d) None of the above.

(v) We require ________ to verify a digital signature.
(a) receiver's public key (b) sender's private key
(c) sender's public key (d) receiver's private key.

(vi) Which of the following step slows the cryptographic algorithm?
(1) Increase in Number of rounds (2) Decrease in Block size
(3) Decrease in Key Size (4) Increase in Subkey Generation
(a) 1 & 3 (b) 2 & 3 (c) 3 & 4 (d) 2 & 4.

(vii) A firewall that uses two TCP connections is
(a) Bastion (b) Application Gateway
(c) Circuit level Gateway (d) Packet Filter.

(viii) ______________ provides privacy, integrity, and authentication in email.
(a) IPSec (b) PGP
(c) SSL (d) None of the above.

(ix) ______________ provides security at the transport layer.
(a) SSL (b) Either SSL or TLS
(c) TLS (d) Both SSL and TLS.

(x) How many keys does the Triple DES algorithm use?
(a) 2 (b) 3 (c) 2 or 3 (d) 3 and 4.

Group – B

2. (a) Use the Playfair Cipher Algorithm to Encrypt the Plain Text "MONARCHY". Consider the key as "INSTRUMENTS".

(b) What do you understand by "Euler Totient Function"?

(c) Find the multiplicative inverse of 11 in Z_{26}.

(d) Find the value of 7^{86}(mod 13) by using Fermat's Little Theorem.

4 + 2 + 4 + 2 = 12

3. (a) Use the Vernam Cipher to generate the cipher text corresponding to the plain text "CRYPTOGRAPHY". Use "GOODMORNING" as the key.

(b) What do you understand by the term "Homophonic Substitution"?

(c) What do you mean by transposition technique? What will be the output of the following plain text if simple columnar transposition technique (single round) is used to encode it?
Plain Text: "meet me at next midnight"
Key: "FANCY"
Also show the decryption technique.

4 + 2 + (2 + 2 + 2) = 12

Group – C

4. (a) Suppose two people, Alice and Bob [traditional names], want to use insecure email to agree on a secret "shared key" that they can use to do further encryption for a long message. Suppose they choose the Diffie Hellman Key exchange Algorithm. Can you figure out their email being a 3rd person? Justify your answer.

(b) What are the four main stages of AES operation?

(c) Explain the Triple DES Algorithm.

(1 + 4) + 4 + 3 = 12

5. (a) What is key distribution problem?

(b) Explain Diffie Helman key exchange algorithm with an example.

(c) Explain man in the middle attack with a suitable example.

2 + 5 + 5 = 12

Group – D

6. (a) Explain the MD5 algorithm with a suitable diagram. How is it different from SHA-1?

(b) What do you understand by the term "Digital Signature"? How is it generated?

(4 + 4) + (2 + 2) = 12

7. (a) Explain the roll of the Authentication Server (AS) and the Ticket Granting Server (TGS) in Kerberos.

(b) What is a Message digest? Explain HMAC algorithm with a suitable diagram.

(3 + 3) + (2 + 4) = 12

Group – E

8. (a) What do you understand by the term "Firewall"? Name and highlight the key features of the different types of firewalls?

(b) Explain the 3 different methods of Biometric Verification.

(c) Explain the operation of PGP using a schematic diagram.

(2 + 3) + 3 + 4 = 12

9. (a) Why is the SSL layer positioned between Application layer and Transport layer?

(b) Briefly explain the Handshake Protocol of SSL.

(c) What is a Buffer Overflow attack on SSL?

2 + 8 + 2 = 12

Department & Section	Submission link:
Sec A and B1	https://classroom.google.com/c/MTIyNDEzMjE0MDgy/a/Mjc0NjkzMjcyMzcx/details
Sec C and B2	https://classroom.google.com/c/MTIyNDE0OTQzNjY2/a/Mjc0NjkzMjcyMzk3/details