2018

CRYPTOGRAPHY AND NETWORK SECURITY

Paper : CS 717

Full Marks : 100

Time : Three hours

The figures in the margin indicate full marks for the questions.

*Attempt **All** the questions.*

1. Answer **any four** from the following :

4×5=20

(a) The following shows the remainders of power of 10, when divided by 13. The pattern will be reported for higher powers.

$10^0 \bmod 13 = 1$, $10^1 \bmod 13 = -3$, $10^2 \bmod 13 = -4$

$10^3 \bmod 13 = -1$, $10^4 \bmod 13 = 3$, $10^5 \bmod 13 = 4$

Using the above information, find the remainder of an integer when divided by 13. Test your method with 691553672.

(b) Eve performs a chosen-plaintext attack on the following ciphertext :

PWUFFOGWCHFDWIWEJOUUNJORSMDW

RHVCMWJUPVCCG

Eve also very briefly obtains access to Alice's computer and has only enough time to type a two-letter plaintext : 'et'. She then tries to encrypt the short plaintext using two different algorithms; because she is not sure which one is the affine cipher.

Algorithm 1 : plaintext : et Ciphertext : →WC

Algorithm 2 : plaintext : et Ciphertext : →WF

Find the plaintext by cryptanalysis of Affine Cipher.

(c) John is reading a mystery book involving. Cryptography. In one part of the book, the author gives a Ciphertext 'CIW' and two paragraphs later tells the reader that this is a 'shift Cipher' and the plaintext is 'yes'. In the next chapter, the hero found a tablet in a cave with 'XViEWYWI' engraved on it. John immediately found the actual meaning of the ciphertext. What type of attack did John launch here ? What is the plaintext ?

(d) Define index of Co-incidence and Mutual index of Co-incidence.

Use Kasiski test to find the length of the key on the following Ciphertext :

LIOMWGFEGGDVWGHHCQUCRHRWAGWIOWQLKGZ
ETKKMEVLWPCZVGTHVTSGXQOVGCSVETQLTJSUM
VWVEUVLXEWSLGFZMVVWLGYHCUSWXQHKVGSH
EEVFLCFDGVSUMPHKIRZDMPHHBVWVWJWIXGFWL
TSHGJOUEEHHVUCFVGOWICQLTJSUXGLW

Get the confirmation of the guess by Index of Coincidence test.

(e) Encrypt the message, 'the house is being sold' using one of the following ciphers. Ignore the space between words. Decrypt the message using the plaintext :

(i) Vignere cipher with key : 'pounds'

(ii) Autokey cipher with key = 7

2. (a) Create a linear feedback shift register with 4 cells in which by $b_4 = b_1 \oplus b_0$. Show the value of output for 10 transitions (shifts) if the seed is $(0010)_2$.

(b) What is the maximum period of an LFSR? The maximum period length of an LFSR is 64. How many bits does the shift register have?

$2 \times 3 = 6$

3. Answer **any three** from the following :

$3 \times 5 = 15$

(a) How many rounds of operations are used in the DES Cipher?

(b) Why does the DES function need an expansion permutation?

(c) Why does the round-key generator need a parity drop permutation in key generation?

(d) What is triple DES? What is triple DES with two keys? What is triple DES with three keys?

4. Prove that there is infinite number of primes in the set of positive integers.   4

5. Answer the following : $2 \times 4 = 8$

(a) What are square roots of 1 mod n if n is 17 (a prime) obtain the roots?

(b) Find the values of
$$\phi(17), \phi(64), \phi(90), \phi(100), \phi(101).$$

6. Briefly explain the idea behind the RSA Cryptosystem. What is the one-way function in this system ? What is the trapdoor in this system ? Define the public and private keys in this system. Describe the security of this system.   7

7. Answer the following :   2×2=4

   (a) Distinguish between message integrity and message authentication.

   (b) Describe the first criterion, the second criterion and the third criterion for a cryptographic hash function.

8. *(a)* What kind of compression function is used in SHA-512 ? Explain.

   (b) Define the RSA digital signature scheme and compare it to the RSA cryptosystem.

                                    2×5=10

9. *(a)* Define the Diffie-Hellman protocol and its purpose.

(b) In a Diffie-Hellman protocol, $g = 7$, $p = 29$, $x = 3$ and $y = 5$; What is the value of the symmetric Key ? What is the value of R_1 and R_2 ?

(c) In the Diffie-Hellman protocol, what happens if x and y have the same value, that is, Alice and Bob accidentally chosen the same number ? Are R_1 and R_2 the same ? Do the session Keys calculated by Alice and Bob have the same value ? Use an example to prove your claims.

$3 \times 2 = 6$

10. Answer the following : $4 \times 5 = 20$

(a) Find all the solutions to the following set of the two linear equations :

$$2x + 3y = 5 \ (mod\ 8)$$

$$x + 6y \equiv 3 \ (mod\ 8)$$

(b) Distinguish between a session and a connection.

(c) Describe how master secret is created from pre-mater secret in SSL.

(d) Describe the components of a virus code. Explain the purpose of the components of the virus. How does the virus protect itself from being detected by anti-virus software ?

───────