53 (CS 717) CRNS

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.

*Answer **all** questions.*

1. Answer ***any five*** questions :

   a. Given $a = 2740$ and $b = 1760$, find the gcd (a, b) by *Extended Euclidean Algorithm* and find the values of s and t. Verify the result using the value of s and t.

   b. What is a *Linear Diophantine Equation* of two variables ? Obtain *the particular* solution using *Extended Euclidean Algorithm*. Find the *particular and general solution* to the following *Linear Diophantine Equation* : $21x + 14y = 35$.

c. Use the property of *mod operator* to prove the remainder of any integer when divided by 3 is the same as the remainder of the sum of its decimal digit. You may consider the number 6371.

d. Find all the *multiplicative inverse* of the members in Z_{10} and verify.

e. Solve the set of following two equations:

$3x + 5y \equiv 4 \pmod 5$

$2x + y \equiv 3 \pmod 5$

What happens to the solution when mod is different in each congruence relation? What is the common mod?

f. Assume that n is a non-negative integer. The following shows the remainders of powers of 10 when divided by 7. Prove that the pattern will be repeated for higher powers: $10^0 \bmod 7 = 1$, $10^1 \bmod 7 = 3$, $10^2 \bmod 7 = 2$, $10^3 \bmod 7 = -1$, $10^4 \bmod 7 = -3$, $10^5 \bmod 7 = -2$. Using the above information, find the remainder of an integer when divided by 7. Test your method with 631453672.

5×5=25

2. a. State Kerckhoff's Principle. Use the additive cipher with key 15 to decrypt the message 'WTAAD'.

b. What is the size of the key domain of an *affine cipher*? Use an *affine cipher* to decrypt the message 'ZEBBW' with the key pair (7, 2) in Z_{26}^* and Z_{26}.

c. Find all the solutions to the following set of the following two linear equations:

$2x + 3y \equiv 5 \pmod 8$

$x + 6y \equiv 3 \pmod 8$

5×3=15

3. Let us define a new *block* cipher. Design a 5 × 5 matrix as a key of characters as in a Playfair cipher. The plaintext "An exercise to solve" to be encrypted and the ciphertext is to be deciphered using the same designed matrix. 10

4. Answer ***any five*** questions:

a. The encryption key in a *transposition* cipher is (3,2,6,1,5,4). Find the *decryption* key.

b. Let us define a *new stream* cipher. The cipher is affine, but the keys depend on the position of the character in the plaintext. If the plaintext character to be encrypted is in position i, we can find the keys as follows:

- *The multiplicative key* is the (i mod 12)th element in Z_{26}^*.
- *The additive key* is the (i mod 26)th element in Z_{26}.

Encrypt the message 'Cryptography is fun' using this new cipher.

c. What is the *order of a group*? How is it different from *order of an element in a group*? How many *cyclic subgroups* can be made from a group $G = < Z_{10}^*, X >$? G has only four elements: 1, 3, 7, 9. Find the elements of these subgroups.

d. Define an *irreducible polynomial.* Show an LFSR with the characteristic polynomial $x^5 + x^2 + 1$. What is the period?

e. In $GF(2^8)$, find the inverse of (x^5) modulo $(x^8+x^4+x^3+x+1)$ using *Extended Euclidean Algorithm.*

f. Suppose that we have a *block* cipher where $n = 64$. If there are 10 ones in the ciphertext, how many trial and error tests does Eve need to do to recover the plaintext from the intercepted ciphertext in each of the following cases: 1. The cipher is designed as a substitution cipher. 2. The cipher is designed as a transposition cipher.

g. The input/output relation in a 2×2 S-box is shown by the following table. Show the table for the *inverse S-box.*

	Input right bit		
		0	1
Input left bit	0	01	11
	1	10	00

7×5=35

5. The plaintext and ciphertext are each 4-bits long the key is 3 bits long. Assume that the function takes the first and third bits, interprets these two bits as a decimal number, squares the number, and interprets the result as a 4-bit binary pattern. Show the results of encryption and decryption if the original plaintext is 0111 and key is 101. 5

6. Explain the *Key generation* algorithm to generate *round key* in *DES.* 10