53 (CS 717) CNWS

2019

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*** from the following : 5×4=20

   (a) The following shows the remainders of powers of 10 when divided by 13. The pattern will be repeated 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 631453672.

Contd.

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

PWUFFOGWCHFDWIWEJOUUNJORSMDWRHVCMWJUPVCCG

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) Is random *mono-alphabetic substitution* for messages up to 20 letters of English alphabet a *perfect cipher*? Justify mathematically.

(d) 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?

(e) Define *Index of Co-incidence* and *Mutual Index of Co-incidence.*

Use *Kasiski* test to find the length of the key on the following cipher text :

LIOMWGFEGGDVWGHHCQUCRHRW
AGWIOWQLKGZETKKMEVLWPCZVGTH
VTSGXQOVGCSVETQLTJSUMVWVEU
VLXEWSLGFZMVVWLGYHCUSWXQHK
VGSHEEVFLCFDGVSUMPHKIRZDMP
HHBVWVWJWIXGFWLTSHGJOUEEHHVU
CFVGOWICQLTJSUXGLW

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

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

(i) *Vignere cipher* with key: 'dollars'

(ii) *Autokey cipher* with key = 7

2. *(a)* Create a *linear feedback shift register* with 4 cells in which $b_4 = b_1 \oplus b_0$. Show the value of output for 20 transitions (shifts) if the seed is $(0001)_2$.

(b) What is *the maximum period* of an *LFSR*? The *maximum period length* of an *LFSR* is 32. How many bits does the shift register have?

2×3=6

3. Answer the following questions :

4×4=16

(a) How many *exclusive-or* 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?

(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 ***any two*** from the following :

2×4=8

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

(b) Find the values of $\varphi(29)$, $\varphi(32)$, $\varphi(80)$, $\varphi(100)$, $\varphi(101)$.

(c) Write the steps involved in the *recommended primality test*. Present the pseudo-code of the algorithm(s) involved in the *recommended primality* test.

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. 6

7. Answer ***any two*** of 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*.

(c) Ignoring the birth month, how many attempts, on average, are needed to find two persons with the same birth date? Assume that all months have 30 days.

8. (a) List the main features of *SHA-512 cryptographic hash function*. What kind of *compression function* is used in *SHA-512*?

(b) Define the *RSA digital signature* scheme and compare it to the *RSA cryptosystem*. 2×5=10

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

(b) In a *Diffe-Hellman protocol*, $g = 7$, $p = 23$, $x = 3$, and $y = 5$; what is the value of the *symmetric key*? What is the value of R_1 and R_2?

(c) In the *Diffe-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. 2×3=6

10. Answer ***any four*** of the following : 4×5=20

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

$$2x + 3y \equiv 5 \pmod 8$$
$$x + 6y \equiv 3 \pmod 8$$

(b) Distinguish between *a session* and a *connection*.

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

(d) Define *security association (SA)* and explain its purpose.

(e) 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*?