SINGAPORE POLYTECHNIC

2013/2014 SEMESTER TWO EXAMINATION

DIPLOMA IN INFOCOMM SECURITY MANAGEMENT

SECOND YEAR FULL-TIME

APPLIED CRYPTOGRAPHY

Time Allowed: 2 Hours

Instructions to Candidates

1. This paper comprises **10** multiple choice questions in Section A and **4** structured questions in Section B.
2. This paper consists of **7** pages (inclusive of cover page).
3. Answer **ALL** questions in Section A and Section B.
4. All answers should be written in the answer booklet provided.
5. Start each question of Section B on a new page.

SECTION A: MULTIPLE CHOICE QUESTIONS (20 marks)

Answer **all** questions. Choose the best answer. Each question carries 2 marks.

1. _________________ uses the transposition technique to protect the confidentiality of information.
   (a) Playfair cipher
   (b) Rail fence cipher
   (c) Vigenère cipher
   (d) Caesar cipher

2. Which of the following statements is NOT true?
   (a) Substitution cipher involves replacement of characters of text with other characters.
   (b) Advanced Encryption Standard (AES) is unconditionally secure.
   (c) Diffusion seeks to make the statistical structure of the plaintext dissipated into long-range statistics of the ciphertext.
   (d) It is desirable that one bit change in the plaintext or the key produces changes in approximately half of the bits in ciphtertext.

3. Which of the following descriptions is NOT true about the Feistel cipher structure?
   (a) Ciphers constructed using this structure are always invertible.
   (b) Feistel cipher structure is used in Data Encryption Standard (DES).
   (c) Feistel cipher structure has strong avalanche effect.
   (d) Encryption and decryption only differ at their key schedules.

4. Which of the following operations is NOT performed in the ShiftRows transformation of Advanced Encryption Standard (AES)?
   (a) 1-byte circular left shift on the second row.
   (b) 2-byte circular right shift on the third row.
   (c) 1-byte circular right shift on the fourth row.
   (d) 2-byte circular left shift on the second row.

5. ________________ does not use feedback as input for the subsequent round of operation.
   (a) Counter (CTR) mode
   (b) Cipher Block Chaining (CBC) mode
   (c) Electronic Code Book (ECB) mode
   (d) Output Feedback (OFB) mode

6. Both symmetric and asymmetric ciphers can be used in _______________.
   (a) encryption/decryption for data secrecy
   (b) digital signature for message authentication
   (c) key exchange for session key distribution
   (d) message authentication code generation

7. The modulus used in Rivest-Shamir-Adlemen (RSA) applications these days should be at least ________ bits long.
   (a) 256
   (b) 512
   (c) 1024
   (d) 2048

8. Singapore passports are now using ______________ to protect the data within the passport from alteration.
   (a) one-time pad
   (b) Advanced Encryption Standard (AES)
   (c) triple Data Encryption Standard (triple DES)
   (d) digital signature

9. Which of the following descriptions is NOT true about Secure Electronic Transaction (SET)?
   (a) Dual signature (DS) links the Order Information (OI) and the Payment Information (PI) of a transaction.
   (b) DS is signed by the customer on the hash of OI.
   (c) SET relies on certificates.
   (d) DS prevents a merchant from forging OI for a given PI.

10. Which service of Pretty Good Privacy (PGP) enhances resistance to cryptanalysis by reducing redundancy?
   (a) Digital signature.
   (b) Message encryption.
   (c) Compression.
   (d) Segmentation and reassembly.

SECTION B: STRUCTURED QUESTIONS (80 marks)

1. (a) (i) Construct the matrix of letters for Playfair cipher, using the key **EFFECTIVE**.

(4 marks)

(ii) Bob sent the ciphertext "**OV QC HQ BK ET CU"** to Alice, which has been encrypted using Playfair cipher with the above key. It is known that if filler is used, the filler is *x*. Help Alice to decrypt the message. (6 marks)

(b) Given the following permutation table on a 9-bit block, complete the inverse permutation table.

Permutation Table

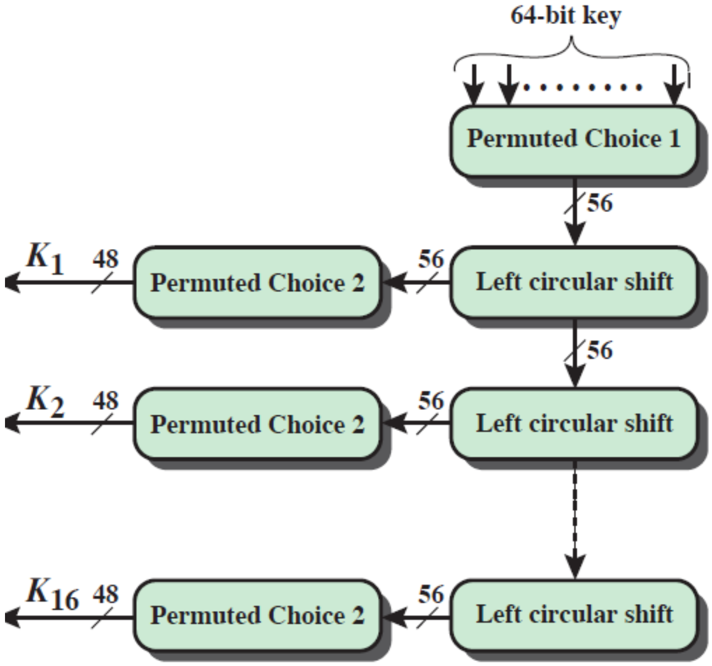
4	9	1
2	6	5
3	7	8

Inverse Permutation Table

3	4	7
8	9	2

(5 marks)

2. (a) Refer to the diagram below of Data Encryption Standard (DES) round key generation. Interpret what is the effect on the round keys if the operation of "left circular shift" is omitted from every round.



(3 marks)

(b) (i) List the four transformations in an Advanced Encryption Standard (AES) round function. (4 marks)

(ii) In an AES round function, identify which transformations provide confusion and which provide diffusion. (6 marks)

(c) (i) Use a diagram to illustrate how DECRYPTION operates in Cipher Block Chaining (CBC) mode. (6 marks)

(ii) If there is a transmission error in the *i*-th ciphertext block C_i, which decrypted plaintext blocks will be affected in CBC and Counter (CTR) modes?

(6 marks)

3. (a) In a public key system using Rivest-Shamir-Adlemen (RSA), you intercept a ciphertext $C = 33$ sent to a user whose public key is $e = 5$, $n = 35$. What is the plaintext M?
(Hint: M is in the range of 2 to 5 inclusive.)
Show clearly the workings of your solution. (8 marks)

(b) Alice and Bob use the Diffie-Hellman key exchange technique with a common prime $q = 23$ and a primitive root $\alpha = 5$.

(i) If Bob has a public key $Y_b = 10$, what is Bob's private key X_b?
(Hint: X_b is in the range of 2 to 4 inclusive.)
Show clearly the workings of your solution. (8 marks)

(ii) If Alice has a public key $Y_a = 8$, and a private key $X_a = 6$, what is the shared key K with Bob?
Show clearly the workings of your solution. (4 marks)

4. (a) Describe two similarities and one difference between hash and Message Authentication Code (MAC) (6 marks)

(b) Explain why digital signature cannot be replaced by MAC? (4 marks)

(c) Describe how the key used for message encryption is distributed in Pretty Good Privacy (PGP). (5 marks)

(d) Part of the Java Application Programming Interface (API) of classes KeyGenerator and Cipher is shown in the table below for your reference. Use the correct methods and parameters to complete the following Java program, which encrypts the message “AAA for Authentication Authorization and Availability” using Advanced Encryption Standard (AES).

Class	Cipher

Fields	static int ENCRYPT_MODE;
	static int DECRYPT_MODE;

Methods	byte[ ] doFinal(byte[ ] data);
	static Cipher getInstance(String transformation);
	byte[ ] getIV( );
	void init(int mode, Key key);
	byte[ ] update(byte[ ] data);

Class	KeyGenerator

Methods	SecretKey generateKey( );
	String getAlgorithm( );
	static KeyGenerator getInstance(String algorithm);
	void init(int keysize);

```
String text = "AAA for Authentication Authorization and Availability";

// Generate a 128-bit AES key
KeyGenerator kg = KeyGenerator.getInstance("AES");
kg.init((i)        );
Key secretkey = kg.(ii)              ( );

// Create a cipher object and initialize it
Cipher cipher = Cipher.(iii)           ("AES/ECB/ PKCS5Padding");
cipher.init((iv)                      ,         );

byte[] plaintext = text.getBytes("UTF8");

// Encrypt the text
byte[] ciphertext = cipher.(v)           (plaintext);
```

(5 marks)

- End of Paper –