

ECE 646 – Fall 2008
Multiple-choice test

1. (1 pt) Arrange the following ciphers in the order of the increasing measure of roughness for the ciphertext obtained by encrypting 1000-letter message with a given cipher (start from the cipher giving the smallest value of the measure of roughness; group together, using an “=” sign, ciphers for which the measure of roughness is the same or very close to each other, e.g. A=B=C, D, E=F, G)
 - A. Rectangle cipher, in which encryption is performed by writing message letters in the rectangle in rows, and reading them in columns, in the order specified by the key.
 - B. Hill cipher with the parameter $d=3$
 - C. general monoalphabetic cipher
 - D. homophonic cipher
 - E. Enigma
 - F. Vigenère cipher with the period $d=3$
 - G. general polyalphabetic cipher with the period $d=3$
 - H. letter-based Vernam cipher with the encryption described by the equation $c_i = m_i + k_i \pmod{26}$, where m_i is a code of the plaintext letter, c_i is a code of the ciphertext letter, and k_i is a code of the keystream letter; the keystream is generated at random and can be used only once.

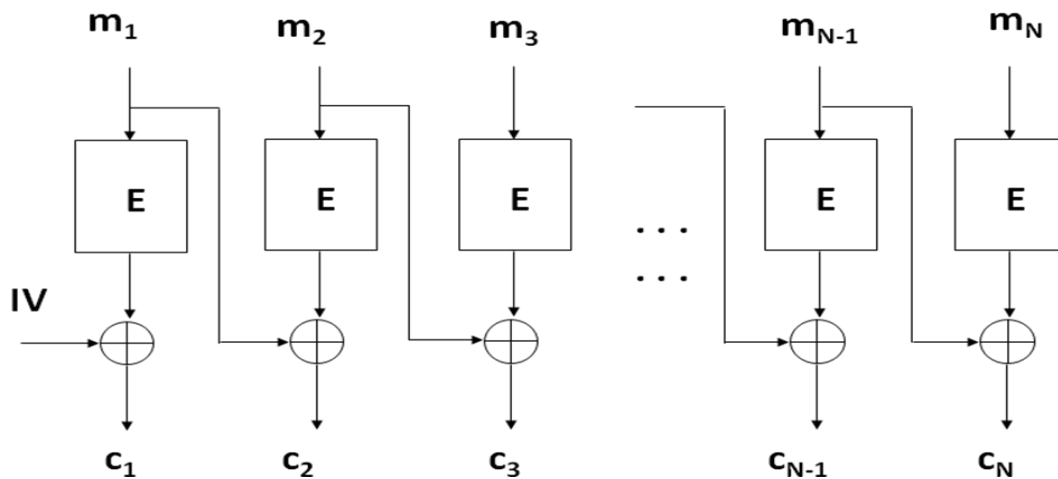
2. (1 pt) In the ciphertext obtained using the Vigenère cipher, a four-character sequence ERTR appears at positions 45, 105, and 441. Additionally, the index of coincidence for this ciphertext is equal to 0.040. Based on this information, the most likely period of the Vigenère cipher is:
 - A. 1
 - B. 2
 - C. 3
 - D. 4
 - E. 6
 - F. 9
 - G. 11
 - H. 12

3. (2 pt) Arrange the following ciphers:
 - a) according to the number of distinct keys (starting from the cipher with the smallest number of keys; if the number of keys is the same, please use the ‘=’ sign, e.g., B=C)
 - b) according to the amount of computations necessary to break the cipher using the best available practical method (starting from the cipher that requires the smallest amount of computations); if the amount of computations is the same, or almost the same, place first the cipher that requires the smaller number of known plaintext blocks

- A. DES in the CBC mode
- B. DES in the OFB mode with $j=64$
- C. Affine cipher
- D. Hill cipher with $d=4$
- E. Playfair cipher
- F. Vigenère cipher with $d=6$
- G. DESX
- H. Letter-based Vernam cipher for the size of the message equal to 20 characters
- I. DES in the CFB mode with $j=8$

Specify your assumptions, if any.

4. (1 pt) The major weaknesses of the inverse CBC mode of DES, for which encryption transformation is given below are that (**more than one answer may be correct**):



- A. decryption is not possible
- B. IV must be kept secret
- C. encryption is more time consuming than decryption
- D. encryption cannot be parallelized
- E. the same plaintext block is always encrypted to the same ciphertext block
- F. the mode is not suitable for a fast random read access to the block m_j
- G. exhaustive key search is easy to mount
- H. analysis of the ciphertext may reveal patterns (e.g., repeating blocks) in the plaintext
- I. decryption circuit takes more area than the encryption circuit

5. (1 pt) Match the following ciphers with the minimum number of plaintext blocks necessary to mount the known-plaintext attack against these ciphers with the probability of success greater than 50%.

- A. DESX in the CFB mode with $j=32$
- B. DES in the CBC mode
- C. DES in the CFB mode with $j=8$
- D. Hill cipher with $d=3$
- E. DES in the counter mode with $j=64$

- a. 1
- b. 2
- c. 4
- d. 8
- e. 9

6. (1 pt) Divide the following transformations performed when exchanging an encrypted only message using PGP, into those
- A. performed only on the sender's side
 - B. performed only on the receiver's side
 - C. performed on both sides
 - D. not performed at either side

Transformations:

- a. generating a random session key
- b. accessing a private key ring
- c. decompression using ZIP algorithm
- d. generating hash value of a message
- e. accessing a public key ring
- f. public key transformation determined by a public key of the receiver
- g. public key transformation determined by a public key of the sender
- h. verifying certificate of the sender

7. (1 pts) Arrange the following ciphers according to the speed of their decryption in hardware assuming that the decryption unit includes 2 DES units working in parallel (start from the cipher that does the decryption in the shortest amount of time)

- A. DESX in the CBC mode
- B. Triple DES in the CBC mode
- C. DES in the CFB mode with $j=16$
- D. DES in the OFB mode with $j=16$
- E. DESX in the counter mode with $j=32$
- F. Triple DES in the counter mode with $j=8$
- G. Triple DES in the OFB mode with $j=8$

Specify your assumptions, if any.

Short problems

1. (3 pts) Break the affine cipher (i.e., find the key (k_1, k_2)) based on the knowledge that the cipher encrypts “E” to “K”, and “I” to “A”; the message is written in English; and the ciphertext starts from the sequence of letters: “TKUX”.
2. (3 pts) Decrypt the ciphertext "EYPXLQNIHJFRVVEVDXMVLI VWVDFZCULTCJKAP" using the Vigenère cipher with the key "CHRIS". Then, encrypt the obtained message using Playfair cipher (following the exact specification given in the Stalling’s book) using the key “WHERE THERE IS A WILL THERE IS A WAY”.
3. (3 pts) Compute the bits number 8, 20, 37, and 55 at the output of the first round of the DESX encryption, assuming that the ciphertext block is equal to $M = 8000000000000001$, the key K_a is equal to “1000000000000008”, and the round key K_1 computed based on the 56-bit key K is equal to “123456789ABC” (all values in the hexadecimal notation; bit no. 1 is the first leftmost bit).
4. (3 pts) Suppose the DES F function mapped every 32-bit input R , regardless of the value of the input K , to 16 leftmost bits of R concatenated with the bitwise-complement of 16 rightmost bits of R , i.e., if $R = R_L \parallel R_R$, then $F(R, K) = R_L \parallel \text{bitwise_complement_of}(R_R)$.

Under the above assumption, express the encryption function of Triple DES using as simple equations as possible. Derive the equations for the corresponding decryption function.

Under the above assumption, are the Triple DES encryption and decryption functions still non-linear functions?

5. (3 pt) Draw a five-level hierarchy of the certification authorities (national central – state - city/county – university – department) that includes the ECE Department at GMU, the department where you have received your undergraduate degree, the Department of Electrical Engineering at UCLA in Los Angeles, California, and the EECS Department at UC Berkeley in Berkeley, California.

Answer the given below questions using the following assumptions:

- Each user registers his/her public key in his/her department
 - During the registration each user receives only his/her certificate and the public key of the departmental CA
 - Each CA issues certificates to all CAs that are connected to it in the hierarchical diagram (both to those above and below it in the hierarchical structure)
 - The notation for a certificate of entity X issued by entity Y is $Y\langle\langle X \rangle\rangle$
 - Each CA issues its own CRLs.
- a. What is a contents of the certification path that needs to be added to the signed only message sent
 - A. by you as a student at GMU to Shilpa from the Department of Electrical Engineering at UCLA
 - B. by Rajesh from the EECS Department at UC Berkeley in Berkeley to Shilpa in the Department of Electrical Engineering at UCLA.
 - b. How many public key operations need to be performed on the sender's side and on the receiver's side for cases A and B, assuming that CRLs are verified during each signature verification ?
 - c. How many private key operations need to be performed on the sender's side and on the receiver's side for cases A and B?
 - d. How many hash function computations need to be performed on the sender's side and on the receiver's side for cases A and B?

Clearly specify any additional assumptions, if any.