# B.Tech. III Semester 6, Global Elective- Cryptography (CS362), Mid Semester Exam March 2022, Section 1

**u19cs012@coed.svnit.ac.in** Switch account

Draft saved

Your email will be recorded when you submit this form

MCQs

Confusion hides the relationship between the ciphertext and the plaintext,

- ○ True
- ◉ False

Clear selection

Compression and expansion P-boxes are,

- ◉ invertible components of block ciphers
- ○ non-invertible components of block ciphers
- ○ linear substitution components of block ciphers
- ○ nonlinear substitution components of block ciphers

Clear selection

Based on the frequency analysis of symmetric cipher you have done in assignment, which are the mos frequently found letters in the English language?

- ○ e,a
- ○ e, o
- ◉ e,t
- ○ e,x

Clear selection

Like DES, AES also uses Feistel Structure

- ○ True
- ◉ False

Clear selection

(403 x 6000 x 5981 x 378)mod 9 equals,

- ○ 7 mod 9
- ○ 3 mod 9
- ◉ 0 mod 9
- ○ 4 mod 9

Clear selection

Chosen Plaintext attack can be carried out when attacker has access to,

- ○ Sender's machine
- ○ Receiver's machine
- ○ Communication channel
- ◉ all of the above

Clear selection

For the same key, a single bit change in a block of plaintext should result in

- ○ a change in exactly half the bits in the block of ciphertext
- ○ a change in half the bits in the block of ciphertext(on average)
- ◉ a change in most of the bits in the block of ciphertext
- ○ a change in a region of ciphertext different from the affected region of plaintext

Clear selection

The irreducible polynomial $x^3 + x^2 + 1$ can be used for the polynomial operations in,

- ◉ GF (2^3)
- ○ GF (2^2)
- ○ GF (2^4)
- ○ None of the above

Clear selection

Inverted permutation table for [6 3 4 5 2 1] is,

- [6 3 4 2 5 1]
- [6 3 4 5 2 1]
- [6 5 2 3 4 1] (selected)
- [1 2 5 4 3 6]

Clear selection

Which of the following attack is the easiest to thwart against ?

- Ciphertext only
- Known Plaintext (selected)
- Chosen Plaintext
- Chosen Ciphertext

Clear selection

Denial by one of the parties in communication can be prevented by

- Denial of Service
- Non-repudiation (selected)
- Entity Authentication
- Message Authentication

Clear selection

In the following mode of operation, a single bit error in transmission may cause many bit errors in that block but no errors in subsequent blocks

- ○ Cipher FeedBack mode
- ○ Cipher Block Chaining mode
- ○ Electronic CodeBook mode
- ◉ all of the above

Clear selection

The order of an element is,

- ◉ a) The order of the cyclic group that it generates
- ○ b) The order of the group
- ○ c) The order of any subgroup of group
- ○ d) Both a) and c)

Clear selection

For a ring R=<Z,+,x>,

- ○ Additive and multiplicative inverse exists for all elements
- ◉ Additive inverse exists for all elements
- ○ Multiplicative inverse exists for all elements
- ○ None of the above

Clear selection

How many rounds does the AES-256 perform?

- ○ 10
- ○ 12
- ◉ 14
- ○ 16

Clear selection

In the DES algorithm the round key is __ bits and the Round Input is __ bits.

- ◉ 48, 64
- ○ 64, 64
- ○ 56, 24
- ○ 32, 32

Clear selection

Alice uses three consecutive permutations [1 3 2]*[3 2 1]*[2 1 3]. Which permutation Bob can use to reverse the process ?( * is the composition operation i.e applying second permutation after the first)

- ◉ [3 2 1]
- ○ [1 2 3]
- ○ [2 3 1]
- ○ [1 3 2]

Clear selection

Difficulty with implementation of One time pad cipher is

- a) key generation
- b) key distribution
- c) both a and b
- d) none of the above

Clear selection

Extended Euclidean algorithm computes greatest common divisor of two numbers 161 and 28 as 7; value of s and t is -1 and 6 respectively. Which of the following is true?

- inverse of 161 in modulus 28 is 6
- inverse of 28 in modulus 161 is 6
- inverse of 161 in modulus 28 is -1
- none of the above

Clear selection

There are ___ elements in $Z_{18}$ while __ elements in $Z_{18^*}$.

- 17, 16
- 18, 17
- 18, 6
- 17, 6

Clear selection

Traffic Analysis can be prevented using,

- ○ hiding frequency of messages
- ○ hiding length of messages
- ○ hiding source and destination of messages
- ◉ all of the above

Clear selection

Ceaser cipher is susceptible to

- ○ ciphertext only attack
- ○ brute force attack
- ○ frequency analysis attack
- ◉ all of the above

Clear selection

The one-time pad is susceptible to,

- ○ known plaintext attack
- ○ chosen plaintext attack
- ○ frequency analysis attack
- ◉ none of the above

Clear selection

The number of subgroups of the group $<Z_{10^*}, x>$

- ○ 1
- ○ 2
- ○ 3
- ◉ 4

Clear selection

There are __ elements in $Z_p$ while __ elements in $Z_p^*$ where p is some prime number.

- ○ p, p
- ◉ p, (p-1)
- ○ (p-1), (p-1)
- ○ (p-1), p

Clear selection

Consider the graph of relative frequency of occurrence of letters in different ciphers viz., Random Polyalphabetic, Vigenere and Playfair. Which one offers better protection against frequency analysis attack? Consider the above graph.

- ◉ a) Vigenere
- ○ b) Playfair

Clear selection

Consider the graph of relative frequency of occurrence of letters in different ciphers viz., Random Polyalphabetic, Vigenere and Playfair. Which of the following do you think is the ideal cipher?

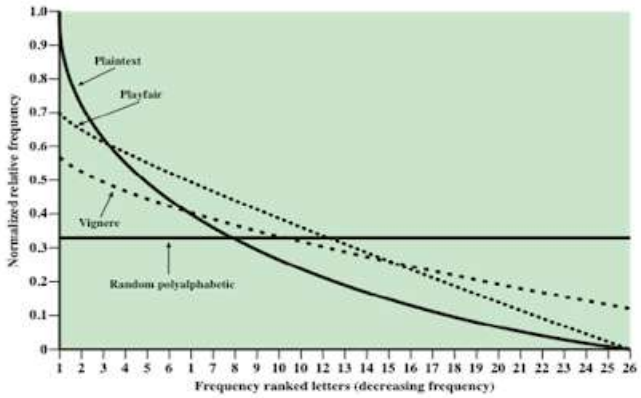


**Figure 3.6 Relative Frequency of Occurrence of Letters**

Courtesy: Crytography and Network Security, William Stallings

- (●) Random Polyalphabetic
- ( ) Vigenere
- ( ) c) Playfair

Clear selection

Modern block ciphers are normally,

- ( ) keyed permutation ciphers
- (●) keyed substitution ciphers
- ( ) non-keyed permutation ciphers
- ( ) non-keyed substitution ciphers

Clear selection

AES suffers from semi-weak keys

- ○ True
- ◉ False

Clear selection

Which of the following is/are invalid size for a finite field?

- ○ 100
- ◉ 89
- ○ 289
- ○ 133

Clear selection

Back Submit Clear form

Never submit passwords through Google Forms.