X

Unit 2 - Week 1

Course outline

How to access the portal?

Week 1

- Lecture 1: Introduction, Caesar cipher
- Lecture 2: Modular Arithmetic, Shift Cipher
- Lecture 3: Classical Ciphers: Affine Cipher and Vigenère Cipher
- Lecture 4: Perfect secrecy and Application on Shift Cipher
- Lecture 5: Problem Discussion on Affine Cipher and Perfect secrecy
- Quiz : Week1_Assignment1
- Assignment Solutions
- Feedback form for Week-1

Week 2

Week 3

Week 4

Week1_Assignment1

The due date for submitting this assignment has passed. Due on 2017-08-07, 23:59 IST.
As per our records you have not submitted this assignment.

1) Let P={0,1,2}, C={1,2,3,4} and for a random key k, e_k and e_k' be two functions from P to C such that $e_k(0)=1$, $e_k(1)=2$, $e_k(2)=4$ and $e_k'(0)=2$, $e_k'(1)=3$, $e_k'(2)=4$ respectively. Choose the correct statement. ***1 point***

- e_k and e_k' both are encryption functions.
- e_k is an encryption function but e_k' is not.
- e_k' is an encryption function but e_k is not.
- e_k and e_k' both are not an encryption functions.

No, the answer is incorrect.
Score: 0

Accepted Answers:
e_k and e_k' both are encryption functions.

2) Which is correct? ***1 point***

- -47 *mod* 16 = 1 and $(-47)^{-1}$ *mod* 16 = 1.
- -47 *mod* 16 = 1, but $(-47)^{-1}$ *mod* 16 does not exist.
- -47 *mod* 16 = 15, but $(-47)^{-1}$ *mod* 16= 15.
- -47 *mod* 16 = 15 and $(-47)^{-1}$ *mod* 16 = 1.

No, the answer is incorrect.
Score: 0

Accepted Answers:
-47 mod 16 = 1 and $(-47)^{-1}$ mod 16 = 1.

3) Let *gcd*(66,255) =*d* and there exist *r,s* ∈ *Z* such that 255*r* + 66*s* =*d*. Pick the correct value of *r,s* and *d*. ***1 point***

- *r* = -7, *s* = 27 and *d* = 3.
- *r* = 7, *s* = 27 and *d* = 3.
- *r* = 7, *s* = -27 and *d* = 3.
- *r* = -7, *s* = -27 and *d* = 3.

No, the answer is incorrect.
Score: 0

Accepted Answers:
r = 7, s = -27 and d = 3.

4) Let r_1 and r_2 be the numbers of all possible keys of affine cipher and Vigenere cipher, respectively, where affine cipher : $\mathscr{P} = \mathscr{C} = \mathbb{Z}_{20}$ and $\mathscr{K}$ ={$(a,b) \in \mathbb{Z}_{20} \times \mathbb{Z}_{20}$: gcd(a,20)=1}, and Vigenere ***1 point***

Cipher: $\mathscr{P} = \mathscr{C} = \mathbb{Z}^4_{20} = \mathscr{K}$. Pick the correct answer.

- r_1 =160 and r_2 =16000.
- r_1 =160 and r_2 =160000.
- r_1 =400 and r_2 =160000.
- r_1 =40 and r_2 =16000.

No, the answer is incorrect.
Score: 0

Accepted Answers:
r_1 =160 and r_2 =160000.

5) Consider a shift cipher with $P = C = Z_{26} = K$.Suppose that "X" is encrypted to "D". Then the encryption of "IAMAGOODBOY" is ***1 po***

- *OGSGMUUJNUE*
- *OGSGQUUJNUE*
- *OGSGMUUJHUE*
- *OGSGMUUJNUF*

No, the answer is incorrect.
Score: 0

Accepted Answers:
OGSGMUUJHUE

6) Consider an affine cipher, where $P = C = Z_{16}$ and $K = \{(a,b) \in Z_{16} \times Z_{16} : gcd(a,16) = 1\}$. If $k = (15,2)$, then ***1 point***

- $e_k(7) = 11$ and $d_k(7) = 11$.
- $e_k(7) = 11$ and $d_k(11) = 11$.
- $e_k(7) = 7$ and $d_k(7) = 11$.
- $e_k(7) = 7$ and $d_k(11) = 11$.

No, the answer is incorrect.
Score: 0

Accepted Answers:
$e_k(7) = 11$ and $d_k(7) = 11$.

7) If an encryption function e_k is identical to the decryption function d_k, then k is said to be an involutary key. Let the set of involutary keys in the shift cipher over Z_{26} is S_1 and in the affine cipher over Z_5 is S_2. Then ***1 point***

- $S_1 = \{0\}$ and $S_2 = \{(1,0), (4,0), (4,1), (4,2), (4,3), (4,4)\}$.
- $S_1 = \{0,13\}$ and $S_2 = \{(1,0), (4,0), (4,1), (4,2), (4,3), (4,4)\}$.
- $S_1 = \{13\}$ and $S_2 = \{(1,0), (4,0)\}$.
- $S_1 = \{0,13\}$ and $S_2 = \{(1,0), (4,0)\}$

No, the answer is incorrect.
Score: 0

Accepted Answers:
$S_1 = \{0,13\}$ and $S_2 = \{(1,0), (4,0), (4,1), (4,2), (4,3), (4,4)\}$.

8) Consider a cryptosystem given by P={a,b}, C={1,2,3,4}, K={k_1, k_2, k_3} and the encryption matrix ***1 point***

	a	b
k_1	1	2
k_2	2	3
k_3	3	4

Pr[X=a]=1/4,Pr[X=b]=3/4, and keys are chosen uniformly at random. The find the correct statement.

- $Pr[X=a|Y=1] = 1$; $Pr[X = a|Y = 2] = 1/3$.
- $Pr[X=a|Y=1] = 1/3$; $Pr[X = a|Y = 2] = 1/9$.
- $Pr[X =a|Y=1] = 1/9$: $Pr[X = a|Y = 2] = 1/9$.
- $Pr[X = a|Y=1] = 1$: $Pr[X = a|Y=2] = 1/4$.

No, the answer is incorrect.
Score: 0

Accepted Answers:
$Pr[X = a|Y=1] = 1$: $Pr[X = a|Y=2] = 1/4$.

9) Here two statements **A** and **B** are given ***1 point***

Statement A:- The affine cipher achieves perfect secrecy if every key is used with equal probability 1/312 .

Statement B:- A cryptosystem (P,C,K,E,D), where $|P| = |C| = |K|$ provides perfect secrecy if every ke used with equal probability $1/|K|$ and for every $x \in P$ and for every $y \in C$ there is a unique key $k \in K$ su that $e_k(x) = y$. Pick the correct option.

- Statement A and Statement B both are true.
- Statement A is true but Statement B is not.
- Statement B is true but Statement A is not.
- Statement A and Statement B both are not true.

No, the answer is incorrect.
Score: 0

Accepted Answers:
Statement A and Statement B both are true.

10) Consider the cryptosystem in which $P = \{a, b, c, d\}$, $C = \{1, 2, 3, 4\}$ and $K = \{k_1,k_2,k_3\}$. ***1 point***

Suppose the encryption matrix is as follows:

	a	b	c	d
k_1	1	2	3	4
k_2	2	3	4	1
k_3	3	4	1	2

Suppose that keys are used with following probabilities,

$Pr[K = k_1] = Pr[K = k_2] = 1/4$, $Pr[K = k_3] = 1/2$ and plaintext distribution is $Pr[X = a] = 1/4$, $Pr[X = b] = 1/2$,
$Pr[X = c] = 1/8 = Pr[X = d]$. Then

- $Pr[Y = 3] = 9/32$ and $Pr[X = a \,|\, Y = 1] = 2/5$
- $Pr[Y = 3] = 5/32$ and $Pr[X = a \,|\, Y = 1] = 2/5$
- $Pr[Y = 3] = 5/16$ and $Pr[X = a \,|\, Y = 1] = 1/5$
- $Pr[Y = 3] = 7/32$ and $Pr[X = a \,|\, Y = 1] = 1/5$

No, the answer is incorrect.
Score: 0

Accepted Answers:
$Pr[Y = 3] = 9/32$ and $Pr[X = a \,|\, Y = 1] = 2/5$

Previous Page End