Applied Cryptography Unit 1 QA Answer Key

Till Double columnar transposition cipher

---

1. **Find the result of the following operations:**
   a. 27 mod 5
   b. 36 mod 12
   c. −18 mod 14
   d. −7 mod 10

Solution

We are looking for the residue r. We can divide the a by n and find q and r. We can then disregard q and keep r.

a. Dividing 27 by 5 results in $r = 2$. This means that $27 \bmod 5 = 2$.
b. Dividing 36 by 12 results in $r = 0$. This means that $36 \bmod 12 = 0$.
c. Dividing −18 by 14 results in $r = -4$. However, we need to add the modulus (14) to make it nonnegative. We have $r = -4 + 14 = 10$. This means that $-18 \bmod 14 = 10$.
d. Dividing −7 by 10 results in $r = -7$. After adding the modulus to −7, we have $r = 3$. This means that $-7 \bmod 10 = 3$.

---

2. Perform the following operations (the inputs come from either Z or Zn):
   a. Add 17 to 27 in Z14.
   b. Subtract 43 from 12 in Z13.
   c. Multiply 123 by −10 in Z19.

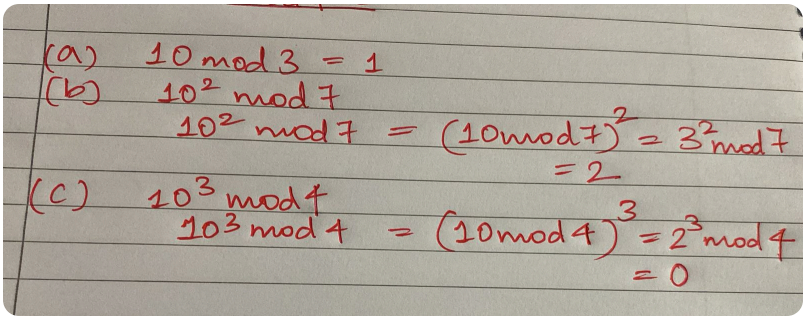
$$
\begin{aligned}
(17 + 27) \bmod 14 &\rightarrow (44) \bmod 14 = 2 \\
(12 - 43) \bmod 13 &\rightarrow (-31) \bmod 13 = 8 \\
(123 \times (-10)) \bmod 19 &\rightarrow (-1230) \bmod 19 = 5
\end{aligned}
$$

---

3. Find the remainder of powers of 10 when divided by an integer.
   a. 10 mod 3

b. 10^2 mod 7

c. 10^3 mod 4



4. Find all additive inverse pairs in Z_{10}.

Solution

The six pairs of additive inverses are (0, 0), (1, 9), (2, 8), (3, 7), (4, 6), and (5, 5). In this list, 0 is the additive inverse of itself; so is 5. Note that the additive inverses are reciprocal; if 4 is the additive inverse of 6, then 6 is also the additive inverse of 4.

---

5. Find all multiplicative inverses in Z_{11}.

Solution:

We have seven pairs: (1, 1), (2, 6), (3, 4), (5, 9), (7, 8), (9, 9), and (10, 10). The integer a in Zn has a multiplicative inverse if and only if **gcd (n, a) ≡ 1 (mod n)**.

---

6. Find the multiplicative inverse of 11 in Z_{26} using Euclidean Algorithm.

Solution

We use a table similar to the one we used before with $r_1 = 26$ and $r_2 = 11$. We are interested only in the value of t.

q	r_1	r_2	r	t_1	t_2	t
2	26	11	4	0	1	−2
2	11	4	3	1	−2	5
1	4	3	1	−2	5	−7
3	3	1	0	5	−7	26
	1	0		−7	26	

The gcd (26, 11) is 1, which means that the multiplicative inverse of 11 exists. The extended Euclidean algorithm gives $t_1 = -7$. The multiplicative inverse is (−7) mod 26 = 19. In other words, 11 and 19 are multiplicative inverse in $\mathbf{Z_{26}}$. We can see that (11 × 19) mod 26 = 209 mod 26 = 1.

---

7. Find the multiplicative inverse of 23 in Z100.

Solution

We use a table similar to the one we used before with $r_1 = 100$ and $r_2 = 23$. We are interested only in the value of t.

q	r_1	r_2	r	t_1	t_2	t
4	100	23	8	0	1	−4
2	23	8	7	1	−4	19
1	8	7	1	−4	9	−13
7	7	1	0	9	−13	100
	1	0		−13	100	

The gcd (100, 23) is 1, which means the inverse of 23 exists. The extended Euclidean algorithm gives $t_1 = -13$. The inverse is $(-13) \bmod 100 = 87$. In other words, 13 and 87 are multiplicative inverses in $\mathbf{Z_{100}}$. We can see that $(23 \times 87) \bmod 100 = 2001 \bmod 100 = 1$.

---

8. A cryptosystem is deemed 'perfectly secure' if the ciphertext provides no information about the plaintext. Which of the following statements about conditional probability best represents this concept?

    1. P(P|C) = P(C)
    2. P(P U C) = P(P)
    3. P(P U C) = P(C)
    4. P(P|C) = P(C)

$P(P|C) = P(P)$

Right answer

This is the correct answer. It states that the conditional probability of a plaintext (P) given a ciphertext (C) is equal to the prior probability of that plaintext (P). In other words, observing the ciphertext provides no additional information about the plaintext.

---

9. A cryptosystem has a vulnerability that gives an attacker a 20% chance of guessing the key if they observe one ciphertext. If the attacker observes two different ciphertexts, and each observation is independent, what is the probability that they will guess the key from one of the two observations?

36%

Right answer

The probability of failure for a single observation is $1 - 0.20 = 0.80$. The probability of failing on both independent observations is $0.80 \times 0.80 = 0.64$. Therefore, the probability of success on at least one observation is $1 - 0.64 = 0.36$, or 36%.

---

10. Which law does the following depict? Explain and give an example where this law is not abided by.

```
Size(Message) == Size(Key) == Size(Ciphertext)
```

```
The law depicted is Shannon's Law of Perfect Secrecy. It states that a cryptosystem is
perfectly secure if and only if the ciphertext provides no information about the plaintext.
This is expressed as:

C=P⊕K

A substitution cipher does not abide by Shannon's Law because the key is a fixed mapping of letters,
which is much smaller than the message. This fixed key is reused for every letter, making the ciphertext
dependent on the plaintext's structure.
```

---

11. Using Caesar cipher, decrypt the ciphertext "WOCCSQYKD" with key = 10.

```
Shift each letter back by 10:
W -> M
O -> E
C -> S
C -> S
S -> I
Q -> G
Y -> O
K -> A
D -> T
Plain Text = MESSIGOAT
```

---

12. Eve has intercepted the ciphertext “UVACLYFZLJBYL”. Show how she can use a brute-force attack to break the cipher.

Solution

Eve tries keys from 1 to 7. With a key of 7, the plaintext is “not very secure”, which makes sense.

Ciphertext: UVACLYFZLJBYL

K = 1	→	**Plaintext:** tuzbkxeykiaxk
K = 2	→	**Plaintext:** styajwdxjhzwj
K = 3	→	**Plaintext:** rsxzivcwigyvi
K = 4	→	**Plaintext:** qrwyhubvhfxuh
K = 5	→	**Plaintext:** pqvxgtaugewtg
K = 6	→	**Plaintext:** opuwfsztfdvsf
K = 7	→	**Plaintext:** notverysecure

---

13. Use Vigenere cipher and encrypt the following text: IMUNDERTHEWATER using key = PLEASEHELP.

The encryption process using the formula $E = (P + K) \pmod{26}$

Plaintext	Key	Plaintext (P)	Key (K)	(P + K) mod 26	Ciphertext
I	P	8	15	23	X
M	L	12	11	23	X
U	E	20	4	24	Y
N	A	13	0	13	N
D	S	3	18	21	V
E	E	4	4	8	I
R	H	17	7	24	Y
T	E	19	4	23	X
H	L	7	11	18	S
E	P	4	15	19	T
W	P	22	15	11	L
A	L	0	11	11	L
T	E	19	4	23	X
E	A	4	0	4	E
R	S	17	18	9	J

---

14. Using the key **CIPHER**, encrypt the plaintext **HELLO** with the Playfair cipher.

- **Key Square**

```
+---+---+---+---+---+
| C | I | P | H | E |
+---+---+---+---+---+
| R | A | B | D | G |
+---+---+---+---+---+
| F | K | L | M | N |
+---+---+---+---+---+
| O | Q | S | T | U |
+---+---+---+---+---+
| V | W | X | Y | Z |
+---+---+---+---+---+
```

- **Plaintext Digraphs**

  The plaintext `HELLO` becomes the digraphs: `HE`, `LX`, `LO`.

Next, we encrypt each digraph using the square.

```
Plaintext  ->  Ciphertext   (Rule Applied)
-----------------------------------------------------
HE         ->  EC           (Same Row)
LX         ->  SP           (Same Column)
LO         ->  FS           (Rectangle)
```

The final combined ciphertext is `ECSPFS`.

---

15. You are to encrypt the plaintext message **ATTACK** using the Hill cipher.Use the following 2×2 matrix as the encryption key K:

$$K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$$

Solution

First, convert the plaintext `ATTACK` into a numerical matrix `P` by grouping it into blocks of two (`AT`, `TA`, `CK`).

$$P = \begin{bmatrix} 0 & 19 \\ 19 & 0 \\ 2 & 10 \end{bmatrix}$$

Next, encrypt by multiplying the plaintext matrix `P` by the key matrix `K`, taking the results modulo 26.

$$C = P \times K \pmod{26}$$

$$\begin{bmatrix} 0 & 19 \\ 19 & 0 \\ 2 & 10 \end{bmatrix}_{\text{P}} \times \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}_{\text{K}} \pmod{26} = \begin{bmatrix} 12 & 17 \\ 5 & 5 \\ 0 & 4 \end{bmatrix}_{\text{C}}$$

Finally, convert the resulting ciphertext matrix `C` back to letters (12=M, 17=R, 5=F, 0=A, 4=E).

The final ciphertext is `MRFFAE`.

---

16. Decrypt the following ciphertext, which was encrypted using the **Rail Fence cipher** with **3 rails**: **DNETLHSEEEDHESWLOTEATLFTAAFCL**

```
D . . . N . . . E . . . T . . . L . . . H . . . S . . . E
. E . E . D . H . E . S . W . L . O . T . E . A . T . L .
. . F . . . T . . . A . . . A . . . F . . . C . . . L .
```

Reading this diagram in a zigzag pattern decrypts the message.

The original plaintext is `DEFENDTHEEASTWALLOFTHECASTLE`.

---

17. Using Columnar transposition cipher, encrypt the plaintext **NEVERGONNAGIVEYOUUP** with key **RICK**.

```
 R   I   C   K
 4   2   1   3
----------------
 N   E   V   E
 R   G   O   N
 N   A   G   I
 G   I   V   E
 Y   O   U   U
```

The encrypted message is `VOGVUEGAIOENIEUNRNGY`.

---

18. Use Double Columnar transposition cipher to encrypt the plaintext **HEREWEGOAGAIN** with key **RUSPA**

Grid 1:

```
 R   U   S   P   A
 3   5   4   2   1
--------------------
 H   E   R   E   W
 E   G   O   A   G
 A   I   N   X   X
```

Grid 2:

```
 R   U   S   P   A
 3   5   4   2   1
--------------------
 W   G   X   E   A
 X   H   E   A   R
 O   N   E   G   I
```

The final encrypted message is `ARIEAGWXOXENGHN`

---

19. If a hacker steals a copy of the database but it's encrypted, has the data's confidentiality been compromised? Explain.

Yes, the data's confidentiality has been compromised. The moment an unauthorized party gains control of the data, the security principle of confidentiality—which ensures data is only accessible to authorized individuals—has been violated, regardless of whether the data is encrypted.

---

20. Your tuition has a test coming up, but your tutor did not send you the material required to prepare for it. Which among the triad does it violate? Now your tutor promises everyone not to reveal your marks in the class, but reveals it anyway. Now which among the triad does this violate?

    The first scenario violates **availability**, as you lack the necessary material to prepare for the test. The second scenario violates **confidentiality**, as your personal information (your marks) was disclosed against the promise to keep it private.

---

21. Why is the one-time pad often cited as the only practical example of a cryptosystem with perfect secrecy? What are its key properties, and what are the major practical limitations?

    The OTP achieves perfect secrecy by following three strict rules:

    - The **key must be as long as the plaintext message**.
    - The key must be **truly random** and not generated by a predictable algorithm.
    - The key must be used **only once** and then destroyed.
      When these conditions are met, an attacker can't break the encryption because for any given ciphertext, every possible plaintext message is equally likely to be the original.
