Cryptography Homework 1

2024 Spring Semester

21 CST H3Art

Exercise 2.1

Evaluate the following:

(a) $7503 \bmod 81$

(b) $(-7503) \bmod 81$

(c) $81 \bmod 7503$

(d) $(-81) \bmod 7503$

> **Solution:**
>
> (a) Since $7503 = 92 \times 81 + 51$, $0 < 51 < 81$, $7503 \bmod 81 = 51$
>
> (b) Since $-7503 = -93 \times 81 + 30$, $0 < 30 < 81$, $(-7503) \bmod 81 = 30$
>
> (c) Since $81 = 0 \times 7503 + 81$, $0 < 81 < 7503$, $81 \bmod 7503 = 81$
>
> (d) Since $-81 = 1 \times 7503 + 7422$, $0 < 7422 < 7503$, $(-81) \bmod 7503 = 7422$

Exercise 2.7

Determine the number of keys in an *Affine Cipher* over $\mathbb{Z}_m$ for $m = 30$, 100 and 1225.

> **Solution:**
>
> To find the prime factors of a number, we used this code below.
>
> ```
> num = int(input())
> prime_factor = []
>
> for i in range(2, num):
>     while True:
>         if num % i == 0:
>             num /= i
>             prime_factor.append(i)
>         else:
>             break
>
> print(prime_factor)
> ```
>
> (a) For $m = 30$, to find the number of keys, we need to factor the prime factors of 30 to get $30 = 2 \times 3 \times 5$. Using the Euler function, we can calculate that there are $\Phi(30) = (2-1)(3-1)(5-1) = 8$ numbers satisfying $\gcd(a, 30) = 1$. The number of keys in an *Affine Cipher* over $\mathbb{Z}_{30}$ is $30 \times 8 = 240$.

(b) For $m = 100$, to find the number of keys, we need to factor the prime factors of 100 to get $100 = 2^2 \times 5^2$. Using the Euler function, we can calculate that there are $\Phi(100) = (2^2 - 2)(5^2 - 5) = 40$ numbers satisfying $\gcd(a, 100)$. The number of keys in an *Affine Cipher* over $\mathbb{Z}_{100}$ is $100 \times 40 = 4000$.

(c) For $m = 1225$, to find the number of keys, we need to factor the prime factors of 1225 to get $1225 = 5^2 \times 7^2$. Using the Euler function, we can calculate that there are $\Phi(1225) = (5^2 - 5)(7^2 - 7) = 840$ numbers satisfying $\gcd(a, 1225)$. The number of keys in an *Affine Cipher* over $\mathbb{Z}_{1225}$ is $1225 \times 840 = 1029000$.

Exercise 2.8

List all the invertible elements in $\mathbb{Z}_m$ for $m = 28$, 33, and 35.

Solution:

To find the factors of a given integer:

```
num = int(input())

for i in range(1, num):
    if num % i == 0:
        print(i)
```

The invertible element a must statisfy $a \in \mathbb{Z}_m$ and $\gcd(a, m) = 1$.

(a) When $m = 28$, since 28's factors are $1, 2, 4, 7, 14$, the invertible elements in $\mathbb{Z}_{28}$ are $1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27$.

(b) When $m = 33$, since 33's factors are $1, 3, 11$, the invertible elements in $\mathbb{Z}_{33}$ are $1, 2, 4, 5, 7, 8, 10, 13, 14, 16, 17, 19, 20, 23, 25, 26, 28, 29, 31, 32$.

(c) When $m = 35$, since 35's factors are $1, 5, 7$, the invertible elements in $\mathbb{Z}_{35}$ are $1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34$.

Exercise 2.9

For $1 \leq a \leq 28$, determine $a^{-1} \bmod 29$ by trial and error.

Solution:

Since 29's factors are only 1 and 29, 29 is a prime. Therefore, for $1 \leq a \leq 28$, all $a^{-1}a \equiv 1 \bmod 29$ have solution.

To determine $a^{-1} \bmod 29$ by trial and error:

```
for i in range(1, 29):
    for j in range(1, 100):
        if (i * j) % 29 == 1:
           print('For {0}, the invert is {1}.'.format(i, j))
            break
```

Finally, all the results are as follows:

```
For 1 , the invert is 1.
For 2 , the invert is 15.
```

```
For 3 , the invert is 10.
For 4 , the invert is 22.
For 5 , the invert is 6.
For 6 , the invert is 5.
For 7 , the invert is 25.
For 8 , the invert is 11.
For 9 , the invert is 13.
For 10 , the invert is 3.
For 11 , the invert is 8.
For 12 , the invert is 17.
For 13 , the invert is 9.
For 14 , the invert is 27.
For 15 , the invert is 2.
For 16 , the invert is 20.
For 17 , the invert is 12.
For 18 , the invert is 21.
For 19 , the invert is 26.
For 20 , the invert is 16.
For 21 , the invert is 18.
For 22 , the invert is 4.
For 23 , the invert is 24.
For 24 , the invert is 23.
For 25 , the invert is 7.
For 26 , the invert is 19.
For 27 , the invert is 14.
For 28 , the invert is 28.
```

Exercise 2.10

Suppose that $K = (5, 21)$ is a key in an *Affine Cipher* over $\mathbb{Z}_{29}$.

(a) Express the decryption function $d_K(y)$ in the form $d_K(y) = a'y + b'$, where a', $b' \in \mathbb{Z}_{29}$

(b) Prove that $d_K(e_K(x)) = x$ for all $x \in \mathbb{Z}_{29}$.

Solution:

(a) Since $e_K(x) = (5x + 21) \bmod 29 = 5x + 21$ and $d_K(y) = a^{-1}(y - b) \bmod 29$, where $a = 5, b = 21$. According to $aa^{-1} \equiv 1 \bmod 29$, the value of a^{-1} is 6. Thus, $d_K(y) = 6(y - 21) \bmod 29 = 6y - 10$.

(b) Proof:

$$\begin{aligned} d_K(e_K(x)) &= a^{-1}(ax + b - b) \bmod 29 \\ &= 6 \times 5x \bmod 29 \\ &= 30x \bmod 29 \\ &= x \end{aligned}$$

Exercise 2.15(a)

Determine the inverses of the following matrices over $\mathbb{Z}_{26}$:

(a) $\begin{pmatrix} 2 & 5 \\ 9 & 5 \end{pmatrix}$

Solution:

Suppose $\mathbf{A} = \begin{pmatrix} 2 & 5 \\ 9 & 5 \end{pmatrix}$, to find $\mathbf{A}^{-1}$ over $\mathbb{Z}_{26}$, we have an equation $\mathbf{A}^{-1} = (\det \mathbf{A})^{-1}\mathbf{A}^*$, where $\mathbf{A}^*$ is adjugate matrix of $\mathbf{A}$.

$$\begin{aligned}\mathbf{A}^* &= \begin{pmatrix} (-1)^{1+1} \times a_{2,2} & (-1)^{1+2} \times a_{1,2} \\ (-1)^{2+1} \times a_{2,1} & (-1)^{2+2} \times a_{1,1} \end{pmatrix} \bmod 26 \\ &= \begin{pmatrix} (-1)^{1+1} \times 5 & (-1)^{1+2} \times 5 \\ (-1)^{2+1} \times 9 & (-1)^{2+2} \times 2 \end{pmatrix} \bmod 26 \\ &= \begin{pmatrix} 5 & -5 \\ -9 & 2 \end{pmatrix} \bmod 26 \\ &= \begin{pmatrix} 5 & 21 \\ 17 & 2 \end{pmatrix}\end{aligned}$$

and for $\det \mathbf{A}$ over $\mathbb{Z}_{26}$:

$$\begin{aligned}\det(\mathbf{A}) &= \det \begin{pmatrix} 2 & 5 \\ 9 & 5 \end{pmatrix} \bmod 26 \\ &= (2 \times 5 - 5 \times 9) \bmod 26 \\ &= -35 \bmod 26 \\ &= 17\end{aligned}$$

Since $17^{-1} \bmod 26 = 23$

$$\begin{aligned}\mathbf{A}^{-1} &= 23\mathbf{A}^* \\ &= 23 \begin{pmatrix} 5 & 21 \\ 17 & 2 \end{pmatrix} \bmod 26 \\ &= \begin{pmatrix} 11 & 15 \\ 1 & 20 \end{pmatrix}\end{aligned}$$

Therefore, the inverse of the matrix $\begin{pmatrix} 2 & 5 \\ 9 & 5 \end{pmatrix}$ over $\mathbb{Z}_{26}$ is $\begin{pmatrix} 11 & 15 \\ 1 & 20 \end{pmatrix}$.

Exercise 2.16

(a) Suppose that π is the following permutation of $\{1, ..., 8\}$:

x	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
$\pi(x)$	4	1	6	2	7	3	8	5

Compute the permutation π^{-1}.

(b) Decrypt the following ciphertext, for a *Permutation Cipher* with $m = 8$, which was encrypted using the key π:

$$\text{TGEEMNELNNTDROEOAAHDOETCSHAEIRLM.}$$

Solution:

(a) The permutation π^{-1} is as follows:

x	1	2	3	4	5	6	7	8
$\pi^{-1}(x)$	2	4	6	1	8	3	5	7

(b) We need to partition the ciphertext into 8 letters per group:

$$\text{TGEEMNEL NNTDROEO AAHDOETC SHAEIRLM.}$$

Next we only need to use $\pi^{-1}(x)$ to get:

$$\text{GENTLEME NDONOTRE ADEACHOT HERSMAIL.}$$

Therefore, the plaintext is:

$$\text{GENTLEMEN DO NOT READ EACH OTHERS MAIL.}$$

Exercise 2.18

Consider the following linear recurrence over $\mathbb{Z}_2$ of degree four:

$$z_{i+4} = (z_i + z_{i+1} + z_{i+2} + z_{i+3}) \bmod 2$$

$i \geq 0$. For each of the 16 possible initialization vectors $(z_0, z_1, z_2, z_3) \in (\mathbb{Z}_2)^4$, determine the period of the resulting keystream.

Solution:

- Start with $(0,0,0,0)$, the keystream is $0,0,0,0,0,0,0,0,0,0,0,0,\cdots$, the period of the resulting keystream is 1.
- Start with $(1,0,0,0)$, the keystream is $1,0,0,0,1,1,0,0,0,1,1,0,\cdots$, the period of the resulting keystream is 5.
- Start with $(0,1,0,0)$, the keystream is $0,1,0,0,1,0,1,0,0,1,0,1,\cdots$, the period of the resulting keystream is 5.
- Start with $(0,0,1,0)$, the keystream is $0,0,1,0,1,0,0,1,0,1,0,0,\cdots$, the period of the resulting keystream is 5.
- Start with $(0,0,0,1)$, the keystream is $0,0,0,1,1,0,0,0,1,1,0,0,\cdots$, the period of the resulting keystream is 5.
- Start with $(1,1,0,0)$, the keystream is $1,1,0,0,0,1,1,0,0,0,1,1,\cdots$, the period of the resulting keystream is 5.
- Start with $(1,0,1,0)$, the keystream is $1,0,1,0,0,1,0,1,0,0,1,0,\cdots$, the period of the resulting keystream is 5.
- Start with $(1,0,0,1)$, the keystream is $1,0,0,1,0,1,0,0,1,0,1,0,\cdots$, the period of the resulting keystream is 5.
- Start with $(0,1,1,0)$, the keystream is $0,1,1,0,0,0,1,1,0,0,0,1,\cdots$, the period of the resulting keystream is 5.
- Start with $(0,1,0,1)$, the keystream is $0,1,0,1,0,0,1,0,1,0,0,1,\cdots$, the period of the resulting keystream is 5.
- Start with $(0,0,1,1)$, the keystream is $0,0,1,1,0,0,0,1,1,0,0,0,\cdots$, the period of the resulting keystream is 5.
- Start with $(1,1,1,0)$, the keystream is $1,1,1,0,1,1,1,1,0,1,1,1,\cdots$, the period of the resulting keystream is 5.
- Start with $(1,1,0,1)$, the keystream is $1,1,0,1,1,1,1,0,1,1,1,1,\cdots$, the period of the resulting keystream is 5.

- Start with $(1, 0, 1, 1)$, the keystream is $1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, \cdots$, the period of the resulting keystream is 5.
- Start with $(0, 1, 1, 1)$, the keystream is $0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, \cdots$, the period of the resulting keystream is 5.
- Start with $(1, 1, 1, 1)$, the keystream is $1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, \cdots$, the period of the resulting keystream is 5.

Exercise 2.23

Suppose we are told that the plaintext

$$\text{breathtaking}$$

yields the ciphertext

$$\text{RUPOTENTOIFV}$$

where the *Hill Cipher* is used (but m is not specified). Determine the encryption matrix.

Solution:

Firstly, we suppose $m = 1$, then $e_{\mathbf{K}}(\text{b}) = e_{\mathbf{K}}(1) = (\text{R}) = (17)$. The encrption equation is as follows:

$$(1)\mathbf{K} = (17)$$

To test whether $\mathbf{K} = (17)$, we also have $e_{\mathbf{K}}(\text{r}) = e_{\mathbf{K}}(17) = (\text{U}) = (20)$, since

$$(17)(17) \bmod 26 = (3) \neq (20)$$

The $\mathbf{K}$ we calculated above is incorrect, $m \neq 1$.

Secondly, suppose $m = 2$, the first two processes of Hill Cipher encryption is as follows:

$$e_{\mathbf{K}}(\text{b}, \text{r}) = e_{\mathbf{K}}(1, 17) = (\text{R}, \text{U}) = (17, 20)$$

$$e_{\mathbf{K}}(\text{e}, \text{a}) = e_{\mathbf{K}}(4, 0) = (\text{P}, \text{O}) = (15, 14)$$

Therefore, we can form a matrix equation:

$$\begin{pmatrix} 1 & 17 \\ 4 & 0 \end{pmatrix} \mathbf{K} = \begin{pmatrix} 17 & 20 \\ 15 & 14 \end{pmatrix}$$

The next thing to do is to find the inverse of $\mathbf{K}$, namely $\mathbf{K}^{-1}$.

However, when we calculate $\det \begin{pmatrix} 1 & 17 \\ 4 & 0 \end{pmatrix} \bmod 26 = (1 \times 0 - 17 \times 4) \bmod 26 = 10$, we cannot find the result of $10^{-1} \bmod 26$, it means $\det \begin{pmatrix} 1 & 17 \\ 4 & 0 \end{pmatrix}$ doesn't have inverse over $\mathbb{Z}_{26}$, m can't be 2.

Nextly, suppose $m = 3$, the first three processes of Hill Cipher encryption is as follows:

$$e_{\mathbf{K}}(\text{b}, \text{r}, \text{e}) = e_{\mathbf{K}}(1, 17, 4) = (\text{R}, \text{U}, \text{P}) = (17, 20, 15)$$

$$e_{\mathbf{K}}(\text{a}, \text{t}, \text{h}) = e_{\mathbf{K}}(0, 19, 7) = (\text{O}, \text{T}, \text{E}) = (14, 19, 4)$$

$$e_{\mathbf{K}}(\text{t}, \text{a}, \text{k}) = e_{\mathbf{K}}(19, 0, 10) = (\text{N}, \text{T}, \text{O}) = (13, 19, 14)$$

We can form another matrix equation:

$$\begin{pmatrix} 1 & 17 & 4 \\ 0 & 19 & 7 \\ 19 & 0 & 10 \end{pmatrix} \mathbf{K} = \begin{pmatrix} 17 & 20 & 15 \\ 14 & 19 & 4 \\ 13 & 19 & 14 \end{pmatrix}$$

Next, assume $\mathbf{A} = \begin{pmatrix} 1 & 17 & 4 \\ 0 & 19 & 7 \\ 19 & 0 & 10 \end{pmatrix}$, we calculate $\det \mathbf{A} = \det \begin{pmatrix} 1 & 17 & 4 \\ 0 & 19 & 7 \\ 19 & 0 & 10 \end{pmatrix} \mod 26 = 19$, since $19^{-1} \mod 26 = 11$, finally we need to find the adjugate matrix $\mathbf{A}^*$ to get $\mathbf{A}^{-1}$:

$$\begin{aligned}
\mathbf{A}^*_{11} &= (-1)^{1+1}(19 \times 10 - 7 \times 0) \mod 26 = 8 \\
\mathbf{A}^*_{12} &= (-1)^{2+1}(17 \times 10 - 4 \times 0) \mod 26 = 12 \\
\mathbf{A}^*_{13} &= (-1)^{3+1}(17 \times 7 - 4 \times 19) \mod 26 = 17 \\
\mathbf{A}^*_{21} &= (-1)^{1+2}(0 \times 10 - 7 \times 19) \mod 26 = 3 \\
\mathbf{A}^*_{22} &= (-1)^{2+2}(1 \times 10 - 4 \times 19) \mod 26 = 12 \\
\mathbf{A}^*_{23} &= (-1)^{3+2}(1 \times 7 - 4 \times 0) \mod 26 = 19 \\
\mathbf{A}^*_{31} &= (-1)^{1+3}(0 \times 0 - 19 \times 19) \mod 26 = 3 \\
\mathbf{A}^*_{32} &= (-1)^{2+3}(1 \times 0 - 17 \times 19) \mod 26 = 11 \\
\mathbf{A}^*_{33} &= (-1)^{3+3}(1 \times 19 - 17 \times 0) \mod 26 = 19
\end{aligned}$$

Therefore, $\mathbf{A}^* = \begin{pmatrix} 8 & 12 & 17 \\ 3 & 12 & 19 \\ 3 & 11 & 19 \end{pmatrix}$

$$\begin{aligned}
\mathbf{A}^{-1} &= 11\mathbf{A}^* \\
&= 11 \begin{pmatrix} 8 & 12 & 17 \\ 3 & 12 & 19 \\ 3 & 11 & 19 \end{pmatrix} \mod 26 \\
&= \begin{pmatrix} 10 & 2 & 5 \\ 7 & 2 & 1 \\ 7 & 17 & 1 \end{pmatrix}
\end{aligned}$$

After finding $\mathbf{A}^{-1}$, the key matrix $\mathbf{K}$ can be found:

$$\begin{aligned}
\mathbf{K} &= \mathbf{A}^{-1} \begin{pmatrix} 17 & 20 & 15 \\ 14 & 19 & 4 \\ 13 & 19 & 14 \end{pmatrix} \\
&= \begin{pmatrix} 10 & 2 & 5 \\ 7 & 2 & 1 \\ 7 & 17 & 1 \end{pmatrix} \begin{pmatrix} 17 & 20 & 15 \\ 14 & 19 & 4 \\ 13 & 19 & 14 \end{pmatrix} \mod 26 \\
&= \begin{pmatrix} 3 & 21 & 20 \\ 4 & 15 & 23 \\ 6 & 14 & 5 \end{pmatrix}
\end{aligned}$$

Let's test whether the $\mathbf{K}$ can encrypt the final three letters "ing" to "INV", namely satisfy $e_K(i, n, g) = e_K(8, 13, 6) = (I, N, V) = (8, 5, 21)$.

$$\begin{pmatrix} 8 & 13 & 6 \end{pmatrix} \begin{pmatrix} 3 & 21 & 20 \\ 4 & 15 & 23 \\ 6 & 14 & 5 \end{pmatrix} \mod 26 = \begin{pmatrix} 8 & 5 & 21 \end{pmatrix}$$

So we can conclude that $m = 3$ and the key matrix $\mathbf{K} = \begin{pmatrix} 3 & 21 & 20 \\ 4 & 15 & 23 \\ 6 & 14 & 5 \end{pmatrix}$.

Exercise 2.30

We describe another stream cipher, which incorporates one of the ideas from the *Enigma* machime used by Germany in World War II. Suppose that π is a fixed permutation of $\mathbb{Z}_{26}$. The key is an element $K \in \mathbb{Z}_{26}$. For all integers $i \geq 1$, the keystream element $z_i \in \mathbb{Z}_{26}$ is defined according to the rule $z_i = (K + i - 1) \bmod 26$. Encryption and decryption are performed using the permutations π and π^{-1}, respectively, as follows:

$$e_z(x) = \pi(x) + z \bmod 26$$

and

$$d_z(y) = \pi^{-1}(y - z \bmod 26)$$

where $z \in \mathbb{Z}_{26}$.

Suppose that π is the following permutation of $\mathbb{Z}_{26}$:

x	0	1	2	3	4	5	6	7	8	9	10	11	12
$\pi(x)$	23	13	24	0	7	15	14	6	25	16	22	1	19

x	13	14	15	16	17	18	19	20	21	22	23	24	25
$\pi(x)$	18	5	11	17	2	21	12	20	4	10	9	3	8

The following ciphertext has been encrypted using this stream cipher; use exhaustive key search to decrypt it:

$$\text{WRTCNRLDSAFARWKXFTXCZRNHNYPDTZ}$$
$$\text{UUKMPLUSOXNEUDOKLXRMCBKGRCCURR}$$

Solution:

Based on the decryption principles of stream cipher and permutation ciphers, I constructed the following Python code, which can help me decrypt using the exhaustive key search:

```python
import math

PI_inv = {
    0: 3, 1: 11, 2: 17, 3: 24, 4: 21, 5: 14, 6: 7, 7: 4, 8: 25, 9: 23, 10: 22,
    11: 15, 12: 19, 13: 1, 14: 6, 15: 5, 16: 9, 17: 16, 18: 13, 19: 12, 20: 20,
    21: 18, 22: 10, 23: 0, 24: 2, 25: 8
}

ciphertext = 'WRTCNRLDSAFARWKXFTXCZRNHNYPDTZUUKMPLUSOXNEUDOKLXRMCBKGRCCURR'

def decrypt(ciphertext: str, K: int) -> str:
    plaintext = []
    for index, ch in enumerate(ciphertext):
        plain_ch = (ord(ch) - 65) - (K + index) % 26
        if plain_ch < 0:
            plaintext.append(chr(PI_inv.get(26 + plain_ch) + 65))
        else:
            plaintext.append(chr(PI_inv.get(plain_ch) + 65))

    return ''.join(plaintext)
```

```python
def main() -> None:
    for K in range(0, 26):
        print('Current K = {0}, the decrypted text is {1}.'.format(K, decrypt(ciphertext, K)))


if __name__ == '__main__':
    main()
```

Running the above code, the output is:

```
Current K = 0, the decrypted text is KJQIXTOKWQSFOXKZFROXOKQWFIFRQKJFVOERWERWIFVTKQQRSFVRWOFICFPW.
Current K = 1, the decrypted text is SFJCZPVSXJUGVZSEGLVZVSJXGCGLJSFGYVHLXHLXCGYPSJJLUGYLXVGCAGWX.
Current K = 2, the decrypted text is UGFAEWYUZFMBYEUHBDYEYUFZBABDFUGBRYODZODZABRWUFFDMBRDZYBAKBXZ.
Current K = 3, the decrypted text is MBGKHXRMEGNTRHMOTIRHRMGETKTIGMBTLRVIEVIEKTLXMGGINTLIERTKSTZE.
Current K = 4, the decrypted text is NTBSOZLNHBQPLONVPCLOLNBHPSPCBNTPDLYCHYCHSPDZNBBCQPDCHLPSUPEH.
Current K = 5, the decrypted text is QPTUVEDQOTJWDVQYWADVDQTOWUWATQPWIDRAORAOUWIEQTTAJWIAODWUMWHO.
Current K = 6, the decrypted text is JWPMYHIJVPFXIYJRXKIYIJPVXMXKPJWXCILKVLKVMXCHJPPKFXCKVIXMNXOV.
Current K = 7, the decrypted text is FXWNROCFYWGZCRFLZSCRCFWYZNZSWFXZACDSYDSYNZAOFWWSGZASYCZNQZVY.
Current K = 8, the decrypted text is GZXQLVAGRXBEALGDEUALAGXREQEUXGZEKAIURIURQEKVGXXUBEKURAEQJEYR.
Current K = 9, the decrypted text is BEZJDYKBLZTHKDBIHMKDKBZLHJHMZBEHSKCMLCMLJHSYBZZMTHSMLKHJFHRL.
Current K = 10, the decrypted text is THEFIRSTDEPOSITCONSISTEDOFONETHOUSANDANDFOURTEENPOUNDSOFGOLD.
Current K = 11, the decrypted text is POHGCLUPIHWVUCPAVQUCUPHIVGVQHPOVMUKQIKQIGVMLPHHQWVMQIUVGBVDI.
Current K = 12, the decrypted text is WVOBADMWCOXYMAWKYJMAMWOCYBYJOWVYNMSJCSJCBYNDWOOJXYNJCMYBTYIC.
Current K = 13, the decrypted text is XYVTKINXAVZRNKXSRFNKNXVARTRFVXYRQNUFAUFATRQIXVVFZRQFANRTPRCA.
Current K = 14, the decrypted text is ZRYPSCQZKYELQSZULGQSQZYKLPLGYZRLJQMGKMGKPLJCZYYGELJGKQLPWLAK.
Current K = 15, the decrypted text is ELRWUAJESRHDJUEMDBJUJERSDWDBRELDFJNBSNBSWDFAERRBHDFBSJDWXDKS.
Current K = 16, the decrypted text is HDLXMKFHULOIFMHNITFMFHLUIXITLHDIGFQTUQTUXIGKHLLTOIGTUFIXZISU.
Current K = 17, the decrypted text is OIDZNSGOMDVCGNOQCPGNGODMCZCPDOICBGJPMJPMZCBSODDPVCBPMGCZECUM.
Current K = 18, the decrypted text is VCIEQUBVNIYABQVJAWBQBVINAEAWIVCATBFWNFWNEATUVIIWYATWNBAEHAMN.
Current K = 19, the decrypted text is YACHJMTYQCRKTJYFKXTJTYCQKHKXCYAKPTGXQGXQHKPMYCCXRKPXQTKHOKNQ.
Current K = 20, the decrypted text is RKAOFNPRJALSPFRGSZPFPRAJSOSZARKSWPBZJBZJOSWNRAAZLSWZJPSOVSQJ.
Current K = 21, the decrypted text is LSKVGQWLFKDUWGLBUEWGWLKFUVUEKLSUXWTEFTEFVUXQLKKEDUXEFWUVYUJF.
Current K = 22, the decrypted text is DUSYBJXDGSIMXBDTMHXBXDSGMYMHSDUMZXPHGPHGYMZJDSSHIMZHGXMYRMFG.
Current K = 23, the decrypted text is IMURTFZIBUCNZTIPNOZTZIUBNRNOUIMNEZWOBWOBRNEFIUUOCNEOBZNRLNGB.
Current K = 24, the decrypted text is CNMLPGECTMAQEPCWQVEPECMTQLQVMCNQHEXVTXVTLQHGCMMVAQHVTEQLDQBT.
Current K = 25, the decrypted text is AQNDWBHAPNKJHWAXJYHWHANPJDJYNAQJOHZYPZYPDJOBANNYKJOYPHJDIJTP.
```

Through observation, we can get that the plaintext should be this row:

```
Current K = 10, the decrypted text is THEFIRSTDEPOSITCONSISTEDOFONETHOUSANDANDFOURTEENPOUNDSOFGOLD.
```

Therefore, the plaintext is as follows:

$$\text{THE FIRST DEPOSIT CONSISTED OF ONE}$$
$$\text{THOUSAND AND FOURTEEN POUNDS OF GOLD}$$