Homework 1
VE475 Introduction to Cryptography

Jiang, Sifan
jasperrice@sjtu.edu.cn
515370910040

May 18, 2019

Ex. 1 - Simple questions

1. Since Alice uses Caesar cipher and we already known the ciphertext, we can apply CCA to decrypt the ciphertext, "EVIRE". So, the 25 possible names of the place are: *duhqd*, *ctgpc*, *bsfob*, *arena*, *zqdmz*, *ypcly*, *xobkx*, *wnajw*, *vmziv*, *ulyhu*, *tkxgt*, *sjwfs*, *river*, *qhudq*, *pgtcp*, *ofsbo*, *neran*, *mdqzm*, *lcpyl*, *kboxk*, *janwj*, *izmvi*, *hyluh*, *gxktg*, or *fwjsf*. However, only "*arena*" and "*river*" are meaningful, which could be the meeting place.

2. Since the length of plaintext *dont* is 4, reasonable size of the key should be 2×2. Label letters as integers from 0 to 25, the plaintext then is $\begin{pmatrix} 3 & 14 & 13 & 19 \end{pmatrix}$ and the ciphertext is $\begin{pmatrix} 4 & 11 & 13 & 8 \end{pmatrix}$. After splitting the letters, we would have

$$\underbrace{\begin{pmatrix} 3 & 14 \\ 13 & 19 \end{pmatrix}}_{A} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 4 & 11 \\ 13 & 8 \end{pmatrix} \mod 26$$

Since $\det(A) = -125$ and $\gcd(-125, 26) = 1$, A is invertible modulo 26. Also, we can obtain that -5 is the multiplicative inverse of -125 modulo 26 by applying extended Euclidean algorithm. We can then calculate

$$\begin{aligned} K = \begin{pmatrix} a & b \\ c & d \end{pmatrix} &\equiv \begin{pmatrix} 3 & 14 \\ 13 & 19 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 4 & 11 \\ 13 & 8 \end{pmatrix} \mod 26 \\ &\equiv \frac{1}{-125} \cdot \begin{pmatrix} 19 & -14 \\ -13 & 3 \end{pmatrix} \cdot \begin{pmatrix} 4 & 11 \\ 13 & 8 \end{pmatrix} \mod 26 \\ &\equiv \frac{1}{-125} \cdot \begin{pmatrix} -106 & 97 \\ -13 & -119 \end{pmatrix} \mod 26 \\ &\equiv \begin{pmatrix} 530 & -485 \\ 65 & 595 \end{pmatrix} \mod 26 \\ &\equiv \begin{pmatrix} 10 & 9 \\ 13 & 23 \end{pmatrix} \mod 26 \end{aligned}$$

So, the encryption matrix is $K = \begin{pmatrix} 10 & 9 \\ 13 & 23 \end{pmatrix}$.

3. We can suppose that $n|b$ is wrong, which gives $b = kn + d$, where k and d are integers and $d \in (0, n)$. Since $n|ab$, we would have $ab = ln$, where l is an integer. After combining

two relations above, we have

$$
\begin{aligned}
a(kn+d) &= ln \\
akn+ad &= ln \\
ad &= (l-ak)n \\
\frac{ad}{n} &= l-ak
\end{aligned}
$$

Since $l-ak$ is an integer, so should $\frac{ad}{n}$ be an integer. However, since $\gcd(a,n)=1$ and $d \in (0,n)$, which gives $n \nmid a$ and $n \nmid d$, $\frac{ad}{n}$ could not be an integer. So, the assumption is wrong and $n|b$.

4. Applying Euclidean algorithm

$$
\begin{aligned}
30030 &= 116 \times 257 + 218 \\
257 &= 1 \times 218 + 39 \\
218 &= 5 \times 39 + 23 \\
39 &= 1 \times 23 + 16 \\
23 &= 1 \times 16 + 7 \\
16 &= 2 \times 7 + 2 \\
7 &= 3 \times 2 + 1 \\
2 &= 2 \times 1
\end{aligned}
$$

So, $\gcd(30030, 257) = 1$.

Since $16^2 = 256 < 257 < 289 = 17^2$, the factor of 257 could only be obtained from 2, 3, 5, 7, 11, and 13. However, none of these primes can exact divide 257. So, 257 is a prime.

5. The main reason it is dangerous is that after applying the same key twice in the OTP, the ciphertext would be the same with the plaintext before encryption.

Ex. 2 -