Data Privacy Homework 3

Daoyu Wang PB21030794

January 1

Contents

1 Permutation Cipher

1.1 (a)

Just need to solve the **inverse permutation** of the mapping x to $\pi(x)$.

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

1.2 (b)

We can devide the ciphertext into blocks of length 8 and then use mapping $\pi^{-1}(x) \sim x$ to decrypt each block as follows:

$$\pi^{-1}\begin{pmatrix} T & G & E & E & M & N & E & L \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ N & N & T & D & R & O & E & O \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ A & A & H & D & O & E & T & C \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ S & H & A & E & I & R & L & M \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix} = \begin{pmatrix} G & E & N & T & L & E & M & E \\ 2 & 4 & 6 & 1 & 8 & 3 & 5 & 7 \\ N & D & O & N & O & T & R & E \\ 2 & 4 & 6 & 1 & 8 & 3 & 5 & 7 \\ A & D & E & A & C & H & O & T \\ 2 & 4 & 6 & 1 & 8 & 3 & 5 & 7 \\ H & E & R & S & M & A & I & L \\ 2 & 4 & 6 & 1 & 8 & 3 & 5 & 7 \end{pmatrix} \tag{1}$$

which can be writed as:

$$\text{GENTLEMENDONOTREADEACHOTHERSMAIL} \tag{2}$$

or

$$\text{GENTLEMEN DO NOT READ EACH OTHERS MAIL.} \tag{3}$$

2 Perfect Secrecy

2.1 (a)

A cryptosystem has a perfect secrecy if

$$\forall m \in M, c \in C, \Pr[M = m] = \Pr[M = m | C = c] \tag{4}$$

which can be explained as the ciphertext c does not give any information about the plaintext m.

Based on **Bayes' theorem**, we have:

$$\Pr[M = m|C = c] = \frac{\Pr[C = c|M = m] \Pr[M = m]}{\Pr[C = c]} \tag{5}$$

Since each key is chosen uniformly at random, so knowing j, there is only one key that encrypts j to a $L(i, j)$ among the n keys (Each number appears once in a column). Concerning $\Pr(c)$, each $L(i, j)$ appears n times in the square among the n^2 possible cases. So $\Pr[C = c|M = m] = \frac{1}{n}$ and $\Pr[C = c] = \frac{n}{n^2}$. Thus, we have:

$$\Pr[M = m|C = c] = \frac{\Pr[M = m] \cdot \frac{1}{n}}{\frac{n}{n^2}} = \Pr[M = m] \tag{6}$$

In conclusion, the Latin Square Cryptosystem achieves perfect secrecy if the key is chosen uniformly at random.

2.2 (b)

Since the Latin Square Cryptosystem achieves perfect secrecy, we have:

$$\Pr[M = m] = \Pr[M = m|C = c] \tag{7}$$

So, we can deduce with the **Bayes' theorem** again:

$$\begin{aligned} \forall c \in C, \Pr[C = c] &= \frac{\Pr[M = m] \cdot \Pr[C = c|M = m]}{\Pr[M = m|C = c]} \\ &= \frac{\Pr[M = m] \cdot \Pr[C = c|M = m]}{\Pr[M = m]} \\ &= \Pr[C = c|M = m] \end{aligned} \tag{8}$$

As $|M| = |C| = |K|$, we know that there is only one key among n that encrypts m to c. So

$$\forall c \in C, \Pr[C = c|M = m] = \frac{1}{n} \tag{9}$$

We can conclude that every ciphertext is equally probable.

3 RSA

3.1 (a)

The public key e can be select by $2 < e < (p - 1)(q - 1)$ and e and $(p - 1)(q - 1)$ are coprime. So there are $\phi((p - 1)(q - 1))$ possible values for e.

Consider that $p = 101$ and $q = 113$, we have:

$$\begin{aligned}\phi((p-1)(q-1)) &= \phi(100 \times 112) \\ &= \phi(2^2 \times 5^2 \times 2^4 \times 7) \\ &= \phi(2^6 \times 5^2 \times 7) \\ &= \phi(2^6) \times \phi(5^2) \times \phi(7) \\ &= 2^5(2-1) \times 5(5-1) \times 6 \\ &= 3840\end{aligned} \tag{10}$$

So there are 3840 possible values for e.

3.2 (b)

The ciphertext c can be calculated by:

$$\begin{aligned}c &= m^e \mod n \\ &= 9726^{3533} \mod 11413 \\ &= 5761\end{aligned} \tag{11}$$

So the ciphertext received by Bob is 5761.
When Bob decrypts the ciphertext, he will do the following steps:

- Calculate the private key.

  Firstly he can calculate $n = pq = 11413$ and then the private key d by the following equation:

$$\begin{aligned}d &= e^{-1} \mod (p-1)(q-1) \\ &= 3533^{-1} \mod 11200 \\ &= 6597\end{aligned} \tag{12}$$

- Calculate the plaintext m by $m = c^d \mod n$. We have:

$$\begin{aligned}m &= c^d \mod n \\ &= 5761^{6597} \mod 11413 \\ &= 9726\end{aligned} \tag{13}$$

3.3 (c)

We know that $\Phi(n) = (p-1)(q-1)$, so if $\Phi(n)$ and n are known, we can calculate p and q by the following equation:

$$\begin{cases} n &= pq \\ \Phi(n) &= (p-1)(q-1) \end{cases} \tag{14}$$

We can rewrite the equation as:

$$\begin{cases} p+q = n - \Phi(n) + 1 \\ pq = n \end{cases} \tag{15}$$

Eliminate the variable q from the equations, we have:

$$p^2 - (n - \Phi(n) + 1)p + n = 0 \tag{16}$$

which is a quadratic equation in the unknown p. And we can compute p and q in polynomial time by solving the above quadratic equation.

4 Multi-Party Computation

4.1 (a)Paillier encryption

4.1.1 Encryption

A simpler variant of the above key generation steps would be to set $g = n+1$ and $\lambda = \Phi(n)$, which makes μ as follows:

$$\begin{aligned} \mu &= (L(g^{\Phi(n)} \mod n^2))^{-1} \mod n \\ &= (L((n+1)^{\Phi(n)} \mod n^2))^{-1} \mod n \\ &= (L(1 + \Phi(n) \cdot n + \sum_{k=2}^{\Phi(n)} \binom{\Phi(n)}{k}) \mod n^2)^{-1} \mod n \\ &= (L((1 + \Phi(n) \cdot n) \mod n^2))^{-1} \mod n \end{aligned} \tag{17}$$

As $1 + \Phi(n) \cdot n = 1 + pq(p-1)(q-1) < (pq)^2 = n^2$ and $L(x) = \frac{x-1}{n}$, we can get:

$$\begin{aligned} \mu &= (L((1 + \Phi(n) \cdot n) \mod n^2))^{-1} \mod n \\ &= (\frac{1 + \Phi(n) \cdot n - 1}{n})^{-1} \mod n \\ &= \Phi(n)^{-1} \mod n \end{aligned} \tag{18}$$

So the public key is $(n, g) = (n, n+1)$ and the private key is $(\lambda, \mu) = (\Phi(n), \Phi(n)^{-1} \mod n)$.

Substitute the given value p, q and r, we can calculate n as $p \cdot q = 11 * 17 = 187$, g as $n + 1 = 188$ and $r = 83$. The ciphertext of $m = 175$ can be calculated by:

$$\begin{aligned} c &= g^m \cdot r^n \mod n^2 \\ &= 188^{175} \cdot 83^{187} \mod 187^2 \\ &= 23911 \end{aligned} \tag{19}$$

4.1.2 Homomorphic Addition of Paillier

$$\begin{aligned} \text{Decrypt}((c_1 \cdot c_2) \mod n^2) &= \text{Decrypt}(g^{m_1} r^n \cdot g^{m_2} r^n \mod n^2) \\ &= \text{Decrypt}(g^{m_1+m_2} (r^2)^n \mod n^2) \end{aligned} \tag{20}$$

As r is a random number, r^2 is also a random number. So we can get:

$$\begin{aligned} \text{Decrypt}((c_1 \cdot c_2) \mod n^2) &= \text{Decrypt}(g^{m_1+m_2} (r^2)^n \mod n^2) \\ &= m_1 + m_2 \end{aligned} \tag{21}$$

4.2 (b)Secret Sharing

Firstly, we know for any bit x, y, $x \oplus x = 0$, $x \oplus 0 = x$ and $x \oplus y = y \oplus x$. So we can use the following algorithm to generate the shares:

$$\begin{aligned} (a_1 \oplus a_2 \oplus a_3) &= (x_3 \oplus v) \oplus (x_1 \oplus v) \oplus (x_2 \oplus v) \\ &= (x_1 \oplus x_2 \oplus x_3) \oplus (v \oplus v \oplus v) \\ &= 0 \oplus v \\ &= v \end{aligned} \tag{22}$$

So in order to compute $v_1 \oplus v_2$, we can compute $(a_1 \oplus a_2 \oplus a_3) \oplus (b_1 \oplus b_2 \oplus b_3)$ as follows:

$$(a_1 \oplus a_2 \oplus a_3) \oplus (b_1 \oplus b_2 \oplus b_3) = v_1 \oplus v_2 \tag{23}$$

5 Computational Security

5.1 (a)

Interchangeable "Interchangeable" means that if two objects are interchangeable, they can be substituted for each other in a scheme without compromising the security.

Indistinguishable "Indistinguishable" means that an adversary cannot distinguish two different inputs or states from each other.

Difference "Interchangeable" emphasizes the substitutablity of objects, while "indistinguishable" focuses the difficulty for an adversary to diffrenciate between these objects.

5.2 (b)

5.2.1 Difinition

A function $f(\lambda)$ is negligible if, for every polynomial function $p(\lambda)$, we have $\lim_{\lambda\to\infty} p(\lambda)f(\lambda) = 0$.

5.2.2 Lemmas

Lemma 1 Before all, we can prove that $\forall a > 1, b > 0$, $\frac{1}{a^{\lambda^b}}$ is negligible because give any polynomial function $p(\lambda) = a_n\lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_1\lambda + a_0$, there exists a function λ^{n+1} and $\lim_{\lambda\to\infty} \frac{p(\lambda)}{\lambda^{n+1}} = 0$ because:

$$\begin{aligned}
\lim_{\lambda\to\infty} \frac{p(\lambda)}{\lambda^{n+1}} &= \lim_{\lambda\to\infty} \frac{a_n\lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_1\lambda + a_0}{\lambda^{n+1}} \\
&= \lim_{\lambda\to\infty} \frac{a_n\lambda^n}{\lambda^{n+1}} + \frac{a_{n-1}\lambda^{n-1}}{\lambda^{n+1}} + \cdots + \frac{a_1\lambda}{\lambda^{n+1}} + \frac{a_0}{\lambda^{n+1}} \\
&= \lim_{\lambda\to\infty} \frac{a_n}{\lambda} + \frac{a_{n-1}}{\lambda^2} + \cdots + \frac{a_1}{\lambda^{n+1}} + \frac{a_0}{\lambda^{n+1}} \\
&= 0
\end{aligned} \tag{24}$$

And also,$\forall a > 1, b > 0$, for $\frac{1}{a^{\lambda^b}}$ and let $\lambda' = \lambda^b$, apply **Lópida's Law** and we have:

$$\begin{aligned}
0 \le \lim_{\lambda\to\infty} \frac{\lambda^{n+1}}{a^{\lambda^b}} &= \lim_{\lambda'\to\infty} \frac{\lambda'^{\frac{n+1}{b}}}{a^{\lambda'}} \\
&\le \lim_{\lambda'\to\infty} \frac{\lambda'^{\lceil\frac{n+1}{b}\rceil}}{a^{\lambda'}} \\
&= \lim_{\lambda'\to\infty} \frac{\lceil\frac{n+1}{b}\rceil!}{a^{\lambda'}(\ln a)^{\lceil\frac{n+1}{b}\rceil}} \\
&= 0
\end{aligned} \tag{25}$$

So for any polynomial function $p(\lambda)$, we have:

$$\begin{aligned}
\lim_{\lambda\to\infty} p(\lambda)\frac{1}{a^{\lambda^b}} &= \lim_{\lambda\to\infty} \frac{p(\lambda)}{\lambda^{n+1}} \cdot \lambda^{n+1}\frac{1}{a^{\lambda^b}} \\
&= 0
\end{aligned} \tag{26}$$

Lemma 2 Also, we can prove that for all $g(\lambda)$, if $\lim_{\lambda\to\infty} g(\lambda) = \infty$, then $\frac{1}{\lambda^{g(\lambda)}}$ is negligible. Because give any polynomial function $p(\lambda) = a_n\lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_1\lambda + a_0$, there exists a function λ^{n+1} and $\lim_{\lambda\to\infty} \frac{p(\lambda)}{\lambda^{n+1}} = 0$.

And also, for $g(\lambda)$ and $\frac{1}{\lambda^{g(\lambda)}}$, we have:

$$\begin{aligned}\lim_{\lambda\to\infty} \lambda^{n+1}\frac{1}{\lambda^{g(\lambda)}} &= \lim_{\lambda\to\infty} \frac{1}{\lambda^{g(\lambda)-n-1}} \\ &= 0\end{aligned} \tag{27}$$

So for any polynomial function $p(\lambda)$, we have:

$$\begin{aligned}\lim_{\lambda\to\infty} p(\lambda)\frac{1}{\lambda^{g(\lambda)}} &= \lim_{\lambda\to\infty} \frac{p(\lambda)}{\lambda^{n+1}} \cdot \lambda^{n+1}\frac{1}{\lambda^{g(\lambda)}} \\ &= 0\end{aligned} \tag{28}$$

So $\frac{1}{\lambda^{g(\lambda)}}$ is negligible.

Lemma 3 Finally, we can prove that $\forall a > 0$, $\frac{1}{\lambda^a}$ is not negligible because give a polynomial function $p(\lambda) = \lambda^{a+1}$, we have:

$$\begin{aligned}\lim_{\lambda\to\infty} \lambda^{a+1}\frac{1}{\lambda^a} &= \lim_{\lambda\to\infty} \frac{\lambda^{a+1}}{\lambda^a} \\ &= \lim_{\lambda\to\infty} \lambda \\ &= \infty\end{aligned} \tag{29}$$

5.2.3 Prove

- $\frac{1}{2^{\lambda/2}}$ is negligible.

$$\frac{1}{2^{\lambda/2}} = \frac{1}{(\sqrt{2})^\lambda} \tag{30}$$

  As $\sqrt{2}$ is greater than 1 and 1 is greater than 0 which corresponds to the case of **Lemma 1**, $\frac{1}{2^{\lambda/2}}$ is negligible.

- $\frac{1}{2^{\log(\lambda^2)}}$ is not negligible.

$$\begin{aligned}\frac{1}{2^{\log(\lambda^2)}} &= \frac{1}{2^{2\log\lambda}} \\ &= \frac{1}{4^{\log\lambda}} \\ &= \frac{1}{\lambda^{\log 4}}\end{aligned} \tag{31}$$

  As $\log 4$ is greater than 0 which corresponds to the case of **Lemma 3**, $\frac{1}{2^{\log(\lambda^2)}}$ is not negligible.

- $\frac{1}{\lambda^{\log\lambda}}$ is negligible.

  As $\lim_{\lambda\to\infty}\log\lambda = \infty$ which corresponds to the case of **Lemma 2**, $\frac{1}{\lambda^{\log\lambda}}$ is negligible.

- $\frac{1}{\lambda^2}$ is not negligible.

  As $2 > 0$ which corresponds to the case of **Lemma 3**, so $\frac{1}{\lambda^2}$ is not negligible.

- $\frac{1}{2^{(\log\lambda)^2}}$ is negligible.

$$\begin{aligned}\frac{1}{2^{(\log\lambda)^2}} &= \frac{1}{2^{\log\lambda\cdot\log\lambda}} \\ &= \frac{1}{\lambda^{\log 2\cdot\log\lambda}}\end{aligned} \tag{32}$$

  As $\lim_{\lambda\to\infty}\log 2\cdot\log\lambda = \infty$ which corresponds to the case of **Lemma 2**, $\frac{1}{2^{(\log\lambda)^2}}$ is negligible.

- $\frac{1}{(\log\lambda)^2}$ is not negligible.

  Select $p(\lambda) = (\log\lambda)^2$, we have:

$$\begin{aligned}\lim_{\lambda\to\infty}\lambda^2\cdot\frac{1}{(\log\lambda)^2} &= \lim_{\lambda\to\infty}\frac{\lambda^2}{(\log\lambda)^2} \\ &= \lim_{\lambda\to\infty}\frac{2\lambda^2}{2\log\lambda} \\ &= \lim_{\lambda\to\infty}2\lambda^2 \\ &= \infty\end{aligned} \tag{33}$$

  So $\frac{1}{(\log\lambda)^2}$ is not negligible.

- $\frac{1}{\lambda^{1/\lambda}}$ is not negligible.

  Select $p(\lambda) = \lambda$, we have:

$$\begin{aligned}\lim_{\lambda\to\infty}\lambda\cdot\frac{1}{\lambda^{1/\lambda}} &= \lim_{\lambda\to\infty}\frac{\lambda}{\lambda^{1/\lambda}} \\ &= \lim_{\lambda\to\infty}\lambda^{1-1/\lambda} \\ &= \infty\end{aligned} \tag{34}$$

  So $\frac{1}{\lambda^{1/\lambda}}$ is not negligible.

- $\frac{1}{\sqrt{\lambda}}$ is not negligible.

  As $\frac{1}{2}$ is greater than 0 which corresponds to the case of **Lemma 3**, $\frac{1}{\sqrt{\lambda}}$ is not negligible.

- $\frac{1}{2^{\sqrt{\lambda}}}$ is negligible.

  As 2 is greater than 1 and $\frac{1}{2}$ is greater than 0 which corresponds to the case of **Lemma 1**, $\frac{1}{2^{\sqrt{\lambda}}}$ is negligible.

5.3 (c)

5.3.1 $f + g$

Since f and g are negligible, we have for any polynomial function $p_1(\lambda)$ and $p_2(\lambda)$:

$$\begin{aligned} \lim_{\lambda\to\infty} p_1(\lambda) \cdot f(\lambda) = 0 \\ \lim_{\lambda\to\infty} p_2(\lambda) \cdot g(\lambda) = 0 \end{aligned} \tag{35}$$

For any polynomial function $p(\lambda)$, select $p_1(\lambda) = p(\lambda)$ and $p_2(\lambda) = p(\lambda)$, we have:

$$\begin{aligned} \lim_{\lambda\to\infty} p(\lambda) \cdot (f(\lambda) + g(\lambda)) &= \lim_{\lambda\to\infty} p(\lambda) \cdot f(\lambda) + p(\lambda) \cdot g(\lambda) \\ &= 0 + 0 \\ &= 0 \end{aligned} \tag{36}$$

So $f + g$ is negligible.

5.3.2 $f \cdot g$

For any polynomial function $p(\lambda)$, select $p_1(\lambda) = p(\lambda)$ and $p_2(\lambda) = 1$, we have:

$$\begin{aligned} \lim_{\lambda\to\infty} p(\lambda) \cdot (f(\lambda) \cdot g(\lambda)) &= \lim_{\lambda\to\infty} (p(\lambda) \cdot f(\lambda)) \cdot (1 \cdot g(\lambda)) \\ &= 0 \cdot 0 \\ &= 0 \end{aligned} \tag{37}$$

5.3.3 f/g

For example, select $f(\lambda) = \frac{1}{2^\lambda}$ and $g(\lambda) = \frac{1}{4^\lambda}$. Obviously, $f(\lambda)$ and $g(\lambda)$ are negligible. But $f(\lambda)/g(\lambda) = 2^\lambda$ is surely not negligible.