# CS6111 (2025): Assignment 1

Instructor: John Augustine

Due: Aug 24, 2025 (11.59 PM IST).

Name: Shri Prathaa M
Roll No: EE22B144

1. (5 marks) In this exercise, we study conditions under which the shift, mono-alphabetic substitution, and Vigenère ciphers are perfectly secret:
   (a) Prove that if only a single character is encrypted, then the shift cipher is perfectly secret.

**Solution:** In Shift Cipher, a message $m = (m_1, m_2, \ldots, m_n)$ gets encrypted using a key $k \in \{0, 1, 2, \ldots\}$ as:

$$Enc_k(m_1, m_2, \ldots) = (m_1 + k \pmod{26},\ m_2 + k \pmod{26},\ \ldots)$$

For a message $m$ of single character,

$$Enc_k(m) = m + k \pmod{26}.$$

Now,

$$Pr[M = m \mid C = c] = Pr[K = m \oplus c \mid C = c] = Pr[K = m \oplus c].$$

As the key is chosen independent of the message and hence independent of the ciphertext.
As the key is chosen uniformly at random (UAR) and there exists only one key such that $k = m \oplus c$,

$$Pr[M = m \mid C = c] = Pr[K = k] = \frac{1}{|K|} = \frac{1}{26}.$$

Also,

$$Pr[M = m] = \sum Pr[M = m \mid C = c].Pr[C = c]$$

$$Pr[M = m] = \sum_{c=0,1,2,\ldots} \frac{1}{26}.Pr[C = c] = \frac{1}{26} \sum_{c=0,1,2,\ldots} Pr[C = c] = \frac{1}{26} \cdot 1 = \frac{1}{26}.$$

Thus, it is proven that knowledge of the ciphertext adds no additional information, i.e.,

$$Pr[M = m \mid C = c] = Pr[M = m].$$

thus proving perfect secrecy.

(b) What is the largest plaintext space $\mathcal{M}$ you can find for which the mono-alphabetic substitution cipher provides perfect secrecy? (Note: $\mathcal{M}$ need not contain only valid English words.)

**Solution:**

Let $\Sigma = \{A, \ldots, Z\}$ be the alphabets in message space and let the key space be $K = S_{26}$, the set of all bijections $\pi : \Sigma \to \Sigma$. The monoalphabetic substitution cipher encrypts a message $m_1 m_2 \cdots m_n \in \Sigma^n$ as $c_i = \pi(m_i)$ for all $i$, using a single (uniformly random) $\pi$.

*Proof of perfect secrecy for $|\mathcal{M}| = 26$ with the message having unique characters:* On fixing any $m, c \in \Sigma$ which doesn't have multiple letters in message space mapping to same letter in Cipher space or vice versa. With $\pi$ uniform over $S_{26}$,

$$Pr[C = c \mid M = m] = \frac{1}{26!}$$

$$Pr[C = c] = \sum Pr[C = c \mid M = m].Pr[M = m] = \frac{1}{26!} \sum Pr[M = m] = \frac{1}{26!}$$

Thus, we have

$$Pr[C = c \mid M = m] = Pr[C = c]$$

By Bayes' rule,

$\Pr[M = m \mid C = c].Pr[C = c] = \Pr[M = m].Pr[C = c \mid M = m]$

$$Pr[M = m \mid C = c] = Pr[M = m].$$

Thus cipher is perfectly secret over $\mathcal{M} = \Sigma$ for message lenth of 26. We can prove this holds for a unique set of characters in message for any message length, $l \leq 26$ using

$$Pr[C = c \mid M = m] = Pr[C = c] = \frac{(26 - l)!}{26!}$$

*$\mathcal{M}$ larger than 26:* $\mathcal{M}$ contains atleast 2 letters that repeat in message, and for a fixed $\pi$,

$$m_1 = m_2 \iff c_1 = c_2, \qquad m_1 \neq m_2 \iff c_1 \neq c_2,$$

since $\pi$ is a bijection. Thus the event $\{c_i = c_j\}$ reveals that $\{m_i = m_j\}$ Therefore perfect secrecy fails for any plaintext space containing messages of length $> 26$. Thus largest message space is 26!

(c) Show how to use the Vigenère cipher to encrypt any word of length $t$ so that perfect secrecy is obtained (note: you can choose the length of the key). Prove your answer.

**Solution:** Let the alphabet be $\Sigma = \{0, 1, \ldots, 25\}$.
For a plaintext $m = (m_1, \ldots, m_t) \in \Sigma^t$, choose a key $k = (k_1, \ldots, k_t) \in \Sigma^t$ uniformly at random and independent of $M$. The Vigenère encryption is

$$c_i \equiv m_i + k_i \pmod{26} \quad \text{for } i = 1, \ldots, t,$$

or in vector form $c \equiv m + k \pmod{26}$.

**Perfect secrecy.** Fix any $m, c \in \Sigma^t$. Then there is a *unique* key $k^\star \in \Sigma^t$ such that $c \equiv m + k^\star \pmod{26}$, namely $k^\star \equiv c - m \pmod{26}$ (coordinate-wise). Since $K$ is uniform on $\Sigma^t$,

$$\Pr[C = c \mid M = m] \;=\; \Pr[K = k^\star] \;=\; \frac{1}{|\Sigma|^t} \;=\; \frac{1}{26^t},$$

which does not depend on $m$.

$$Pr[C = c] = \sum_{m \in M} \Pr[C = c \mid M = m].Pr[M = m] = \frac{1}{26^t} \sum_{m \in M} Pr[M = m] = \frac{1}{26^t}$$

Hence, for all $m, c$,

$$\Pr[M = m \mid C = c] \;=\; \Pr[M = m],$$

by Bayes' rule.

2. (5 marks) Let $G$ be a pseudorandom generator with a polynomial expansion factor $\ell(n)$. In each of the following cases, say whether the defined $G'$ is necessarily a pseudorandom generator. If yes, give a proof; if not, show a counterexample.

(a) Define $G'(s) = G\left(s_1 \cdots s_{\lfloor log(n) \rfloor}\right)$, where $s = s_1 \cdots s_n$.

**Solution:** The modified generator $G'$ only uses the first $\lfloor \log n \rfloor$ bits of the seed $s$. Thus $G'$ effectively has seed length $m = \lfloor \log n \rfloor$, which means there are only $2^m \leq n$ possible outputs.
We can now construct a distinguisher $D$ against $G'$ as,

1. Compute the set
$$\mathcal{L} = \{G(u) \mid u \in \{0,1\}^m\}.$$
2. On input $w \in \{0,1\}^{\ell(n)}$, check if $w \in \mathcal{L}$.

3. If yes, output 1 (guess "pseudorandom"); otherwise output 0 (guess "uniform random").

If $w$ comes from $G'(U_n)$, then $w \in \mathcal{L}$ with probability 1. Hence

$$\Pr[D(G'(U_n)) = 1] = 1.$$

If $w \leftarrow U_{\ell(n)}$ is uniform, then the probability that $w \in \mathcal{L}$ is

$$\Pr[D(U_{\ell(n)}) = 1] = \frac{|\mathcal{L}|}{2^{\ell(n)}} = \frac{2^m}{2^{\ell(n)}} \leq \frac{n}{2^{\ell(n)}} \approx \text{negl}(n).$$

Thus the advantage is

$$\left| \Pr[D(G'(U_n)) = 1] - \Pr[D(U_{\ell(n)}) = 1] \right| = 1 - \text{negl}(n)$$

Therefore $G'$ cannot be pseudorandom. □

(b) Define $G'(s) = G\left(x_1 \cdots x_n\right)$, where $x = G(s)$ and $s = s_1 \cdots s_n$.

**Solution:**
Let $x = G(s)$. Since $G$ is a PRG, $x$ is computationally indistinguishable from $U_{\ell(n)}$. Let $z$ denote the first $n$ bits of $x$. Then:

- If $x \sim G(U_n)$, then $z = x_1 \ldots x_n$.
- If $x \sim U_{\ell(n)}$, then $z \sim U_n$.

Thus $z$ is indistinguishable from uniform $U_n$ because truncation is an efficient mapping of pseudorandom strings. (Truncation to n bits of string pseudorandom to $U_{\ell(n)}$ gives string pseudorandom to $U_n$ )
Now, $G'(s) = G(z)$. Let

$$H_0 = G(x_1 \ldots x_n), \quad H_1 = G(U_n).$$

Since $x_1 \ldots x_n \approx_c U_n$, we have $H_0 \approx_c H_1$. Also $H_1 = G(U_n)$ is pseudorandom by definition of $G$. Hence $H_0$ is pseudorandom as well.
Therefore $G'$ is a PRG. □

3. (5 marks) Consider the following modification to the one-time pad. Let the message $m$ be of length $n$.

**Gen:** Take two distinct integers $i$ and $j$ uniformly at random from $0 \leq i, j \leq 2^{\frac{n}{2}}$, output $k = 2^{\frac{n}{2}} i + j$.

**Enc:** For a given message $m$ and key $k$, output $m \oplus k$.

Is this scheme perfectly secure?

**Solution:** Gen chooses $i \neq j$ uniformly in $[0, 2^{n/2}]$ and sets $k = 2^{n/2}i + j$, then $\text{Enc}(m) = m \oplus k$.
Thus the key is chosen uniformly from $2^n - 2^{n/2}$ combinations ($|\mathcal{K}| < |\mathcal{M}|$)
From Theorem 2.10, the scheme is not perfectly secure.
Let us choose $m_0 = 0^n$ and a ciphertext c with first and second half equal.

$$Pr[M = m_0/C = c] = Pr[K = c \oplus m_0] = Pr[K = c] = 0$$

(As c has first and second half equal and key space doesn't include it) Now lets choose a message $m_1$ with $0^{n-1}1$

$$Pr[M = m_1/C = c] = Pr[K = c \oplus m_1] = \frac{1}{2^n - 2^{n/2}}$$

As the key $c \oplus m$ has unequal halves. Thus

$$Pr[M = m_0/C = c] \neq Pr[M = m_1/C = c]$$

4. (5 marks) In certain practical scenarios, we might be open to compromising with the "perfect" security and allow a little relaxation bound $\epsilon$ to it. We say that the scheme $\Pi$ with security parameter $n$ and message space $\mathcal{M} = \{0,1\}^n$ is almost perfect if

$$\Pr\left[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1\right] \leq \frac{1}{2} + \varepsilon.$$

for some non-zero $\epsilon$.

Consider the one-time pad with key space $\mathcal{K} \subset \{0,1\}^n$. What would be the minimum size of $\mathcal{K}$ as a function of the size of the message space and $\epsilon$ that will assure almost perfect security?

**Solution:** We have message space $\mathcal{M} = \{0,1\}^n$ and consider the one-time pad but with a restricted key-space $\mathcal{K} \subseteq \{0,1\}^n$. Encryption of a message $m$ is

$$\mathsf{Enc}_k(m) = m \oplus k$$

On fixing two distinct messages $m_0, m_1 \in \mathcal{M}$ and let $\Delta = m_0 \oplus m_1 \neq 0$. For any $m$ the ciphertext distribution when encrypting $m$ is the uniform distribution over the set

$$S_m \;=\; m \oplus \mathcal{K} \;=\; \{\, m \oplus k : k \in \mathcal{K} \,\},$$

which has size $|S_m| = |\mathcal{K}|$. ($|S_m| \leq |\mathcal{K}|$ if its any scheme, not jyst one time pad)

$$\Pr\left[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1\right]$$
$$= Pr[b = 0].Pr[A \ outputs \ 0/b = 0] + Pr[b = 1].Pr[A \ outputs \ 1/b = 1]$$
$$= \frac{1}{2}.Pr[A \ outputs \ 0/b = 0] + \frac{1}{2}.Pr[A \ outputs \ 1/b = 1]$$

Let us take 2 mesages $m_0$, $m_1$. If $|S_{m_0}|$ and $|S_{m_1}|$ have ciphertexts that have non-overlapping elements. These elements if gotten as obtained ciphertext, it can be decrypted with probability, 1

Let

$$I = S_{m_0} \cap S_{m_1}$$

Now,

$$Pr[A \ outputs \ 0/b = 0] = 1/2. \Pr[c \in I] + 1. \Pr[c \in I^{'}]$$

$$|I| = |S_{m_0} \cap S_{m_1}| = |S_{m_0}| + |S_{m_1}| - |S_{m_0} \cup S_{m_1}|$$

As $|S_{m_0} \cup S_{m_1}| \leq |M|$, $|S_{m_0}| = |K|$, $|S_{m_1}| = |K|$,

$$|I| \geq |K| + |K| - |M|$$

$$|I^{'}| \leq |K| - (2|K| - |M|) = |M| - |K|$$

As,

$$Pr[A \ outputs \ 0/b = 0] \leq 1/2.(1 - \Pr[c \in I^{'}]) + 1. \Pr[c \in I^{'}]$$

$$Pr[A \ outputs \ 0/b = 0] \leq 1/2 + 1/2.\frac{|M| - |K|}{|K|}$$

$$= \frac{|M|}{2|K|}$$

By symmetry,

$$Pr[A \ outputs \ 1/b = 1] \leq \frac{|M|}{2|K|}$$

Thus,

$$\Pr\left[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1\right] \leq (\frac{1}{2} + \frac{1}{2})\frac{|M|}{2|K|}$$

Thus the value of $\epsilon$ for

$$\Pr\left[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1\right] \leq \frac{1}{2} + \varepsilon.$$

is

$$\frac{|M|}{2|K|} \leq \frac{1}{2} + \varepsilon$$

Thus,

$$\frac{|M|}{2|K|} \leq \frac{1+2\varepsilon}{2}$$

$$|K| \geq \frac{|M|}{1+2\varepsilon}$$

5. (5 marks) Let $G_1, G_2 : \{0,1\}^n \to \{0,1\}^\ell$ be two functions. Define a new generator

$$G : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^\ell : G(s_1, s_2) = G_1(s_1) \oplus G_2(s_2).$$

Suppose if $G$ is not a PRG. Then, prove that neither $G_1$ nor $G_2$ are PRGs.

**Solution:**

Let us assume by contradiction that either $G_1$ or $G_2$ is a secure PRG and that $G$ is not a PRG.

If $G$ is not a PRG, then there exists a probabilistic polynomial-time (PPT) distinguisher $D$ and a non-negligible function $\varepsilon(n)$ such that

$$\Big|\Pr[D(G(s_1, s_2)) = 1] - \Pr[D(r) = 1]\Big| \;\geq\; \varepsilon(n),$$

where $s_1, s_2 \leftarrow \{0,1\}^n$ are independent seeds and $r \leftarrow \{0,1\}^\ell$ is a truly random $\ell$-bit string. Let $r_1, r_2 \leftarrow \{0,1\}^\ell$ be independent uniform strings such that $r = r_1 \oplus r_2$. Now consider

$$\Delta = \Big|\Pr[D(G(s_1, s_2)) = 1] - \Pr[D(r) = 1]$$

$$\Delta = \Big|\Pr[D(G_1(s_1) \oplus G_2(s_2)) = 1] - \Pr[D(r_1 \oplus r_2) = 1]\Big|.$$

By the triangle inequality,

$$\Delta \leq \Big|\Pr[D(G_1(s_1) \oplus G_2(s_2)) = 1] - \Pr[D(r_1 \oplus G_2(s_2)) = 1]\Big| + \Big|\Pr[D(r_1 \oplus G_2(s_2)) = 1] - \Pr[D(r_1 \oplus r_2) = 1]\Big|.$$

Since $\Delta$ is non-negligible, at least one of the two terms on the right must be non-negligible.

Case 1: Assume $G_1$ is PRG

The first term can be used to build a distinguisher $D_1$ for $G_1$. $D_1$ on input y computes $D(y \oplus G_2(s_2))$ (for a random $s_2$) and outputs the result. However $D_1$ has negligible

advantage in distinguishing $G_1(s_1)$ from $r_1$ if it is a PRG. Thus $G_2$ should not be PRG to get a non-negligible term. However, $s \oplus r$ where r is drawn uniformly gives string at UAR. Similarly, $G_1(s_1) \oplus G_2(s_2)$ for $G_1$ being Pseudorandom would make output of $G$ PRG which is a contradiction.

Case 2: Assume $G_2$ is PRG

The second term can be used to build a distinguisher $D_2$ for $G_2$. $D_2$ on input z computes $D(r_1 \oplus z)$ for a random $r_1$ and outputs the result. $D_2$ can't distinguish $G_2(s_2)$ from $r_2$ with non-negligible probability if $G_2$ is a PRG. Thus $G_1$ should not be PRG. Similarly, $G_1(s_1) \oplus G_2(s_2)$ for $G_2$ being Pseudorandom would make output of $G$ PRG which is a contradiction.

Thus G is not a PRG then neither $G_1$ nor $G_2$ should be a PRG.

6. (5 marks) Consider the following definition of perfect secrecy for the encryption of two messages. An encryption scheme $(\text{Gen}, \text{Enc}, \text{Dec})$ over a message space $\mathcal{M}$ is perfectly-secret for two messages if for all distributions over $\mathcal{M}$, all $m, m' \in \mathcal{M}$, and all $c, c' \in \mathcal{C}$ with $\Pr[C = c \wedge C' = c'] > 0$:

$$\Pr[M = m \wedge M' = m' \mid C = c \wedge C' = c'] = \Pr[M = m \wedge M' = m'],$$

where $m$ and $m'$ are sampled independently from the same distribution over $\mathcal{M}$. Prove that no encryption scheme satisfies this definition. (*Hint:* Take $m \neq m'$ but $c = c'$.)

**Solution:** Let us consider $c = c^{'}$ but $m \neq m'$. Now,

$$Pr[M = m \wedge M' = m' \mid C = c \wedge C' = c'] = 0$$

This is because if two messages m and $m^{'}$ give the same ciphertext,c then $Dec_k(c) = m$ and

$$Dec_k(c^{'}) = Dec_k(c) = m^{'}$$

. However this is a contradiction as $m \neq m'$. The probability

$$\Pr[M = m \wedge M' = m'] = \Pr[M = m].\Pr[M' = m']$$

as m and $m^{'}$ are chosen independently. However this can't be zero for all distributions over $\mathcal{M}$ as there exists some distribution with non-zero probability for the messages $m$ and $m^{'}$

# Acknowledgment

I would like to thank Swathi Shree (EE222B149) for useful discussion on solving the problems.