CS60065: Cryptography and Network Security Total: 40 *points*

Assignment 2

Name: Anit Mangal Due: *11.59 pm, Aug 20, 2024*

Note: The basic policies are stated in the course page. Using GPT (or similar tools) to solve problems from the assignment is **strictly prohibited**. Use of any other (possibly online) source(s) **must** be clearly stated in the solution. **Any dishonesty, if caught, will yield zero credits for the entire assignment.**

A. [Perfect Secrecy : $4 \times 4 = 16$ points.]

Answers

A.1 Assuming perfect secrecy holds if for **any** probability distribution over $\mathbf{M}$ and $\mathbf{K}$, every ciphertext $\mathsf{C} \in \mathbf{C}$ and every message $\mathsf{M}_1, \mathsf{M}_2 \in \mathbf{M}$:

$$\Pr[M_R = \mathsf{M}_1 | C_R = \mathsf{C}] = \Pr[M_R = \mathsf{M}_2 | C_R = \mathsf{C}] \tag{1}$$

Since perfect secrecy holds,

$$\begin{aligned} \Pr[M_R = \mathsf{M}_1 | C_R = \mathsf{C}] &= \Pr[M_R = \mathsf{M}_1] \\ \Rightarrow \Pr[M_R = \mathsf{M}_1] &= \Pr[M_R = \mathsf{M}_2] \qquad \text{(From (1))} \end{aligned}$$

+4 bonus

But, our assumption is that perfect secrecy would hold for any probability distribution. This contradicts our assumption. So, our assumption is wrong.
Hence, $\Pr[M_R = \mathsf{M}_1 | C_R = \mathsf{C}] = \Pr[M_R = \mathsf{M}_2 | C_R = \mathsf{C}]$ does not imply perfect secrecy.

A.2 $\forall\, \mathsf{C}_1, \mathsf{C}_2 \in \mathbf{C}$

$$\begin{aligned} \Pr[\mathbf{C}_R = \mathsf{C}_1] &= \sum_{\mathsf{K} \in \mathbf{K}} \Pr[\mathbf{K}_R = \mathsf{K}] \Pr[\mathbf{M}_R = D_{\mathsf{K}}(\mathsf{C}_1)] && \text{(Total Probability)} \\ &= \sum_{\mathsf{K} \in \mathbf{K}} \frac{1}{|\mathbf{K}|} \Pr[\mathbf{M}_R = D_{\mathsf{K}}(\mathsf{C}_1)] && \text{(Using Shannon's Theorem)} \\ &= \frac{1}{|\mathbf{K}|} \sum_{\mathsf{K} \in \mathbf{K}} \Pr[\mathbf{M}_R = D_{\mathsf{K}}(\mathsf{C}_1)] \end{aligned}$$

Using Shannon's Theorem, for every $\mathsf{M} \in \mathbf{M}$ and for every $\mathsf{C} \in \mathbf{C}$, there is a unique key K such that $E_{\mathsf{K}}(\mathsf{M}) = \mathsf{C}$. So, for every $\mathsf{K} \in \mathbf{K}$ and for every $\mathsf{C} \in \mathbf{C}$, there is a unique plaintext M such that $E_{\mathsf{K}}(\mathsf{M}) = \mathsf{C}$. And since $|\mathbf{K}| = |\mathbf{M}|$, every M is utilised if every K is utilised.

$$\begin{aligned} &= \frac{1}{|\mathbf{K}|} \sum_{\mathsf{M} \in \mathbf{M}} \Pr[\mathbf{M}_R = \mathsf{M}] \\ &= \frac{1}{|\mathbf{K}|} \end{aligned}$$

Similiarly,

$$\Pr[\mathbf{C}_R = \mathsf{C}_2] = \frac{1}{|\mathbf{K}|} = \Pr[\mathbf{C}_R = \mathsf{C}_1]$$

+4

$\therefore$ Every ciphertext is equally probable.

A.3 For Affine Cipher, $\mathsf{K} = (a, b) : gcd(a, 26) = 1$
For any $y \in \mathbb{Z}_{26}$,

$$\begin{aligned}
\Pr[\mathbf{C}_R = y] &= \sum_{\mathsf{K} \in \mathbb{Z}_{26}^* \times \mathbb{Z}_{26}} \Pr[\mathbf{K}_R = \mathsf{K}] \Pr[x = D_{\mathsf{K}}(y)] \\
&= \frac{1}{312} \sum_{\mathsf{K} \in \mathbb{Z}_{26}^* \times \mathbb{Z}_{26}} \Pr[x = a^{-1}(y - b) \pmod{26}] \quad \text{(Key is sampled uniformly at random)} \\
&= \frac{1}{312} \sum_{\mathsf{K} \in \mathbb{Z}_{26}^* \times \mathbb{Z}_{26}} \frac{1}{26} \\
&= \frac{1}{312} \cdot \frac{312}{26} \\
&= \frac{1}{26}
\end{aligned}$$

Now, $\forall x, y \in \mathbb{Z}_{26}$,

$$\begin{aligned}
\Pr[\mathbf{C}_R = y | \mathbf{M}_R = x] &= \Pr[\mathbf{K}_R = (a, b) : y = ax + b \pmod{26}] \\
&= \frac{1}{26} \qquad \text{(For an } a\text{, there is a fixed } b \in \mathbb{Z}_{26}\text{)}
\end{aligned}$$

+4 Since $\Pr[\mathbf{C}_R = y | \mathbf{M}_R = x] = \Pr[\mathbf{C}_R = y]$, Affine Cipher achieves perfect secrecy when keys are sampled uniformly at random

A.4 For any $y \in \{0, 1\}^n$,

$$\begin{aligned}
\Pr[\mathbf{C}_R = y] &= \sum_{\mathsf{K} \in \{0,1\}^n \setminus 0^n} \Pr[\mathbf{K}_R = \mathsf{K}] \Pr[x = D_{\mathsf{K}}(y)] \\
&= \frac{1}{2^n - 1} \sum_{\mathsf{K} \in \{0,1\}^n \setminus 0^n} \Pr[x = y \oplus \mathsf{K}] \qquad \text{(Key is sampled uniformly at random)} \\
&= \frac{1}{2^n - 1} \sum_{\mathsf{K} \in \{0,1\}^n \setminus 0^n} \frac{1}{2^n} \\
&= \frac{1}{2^n - 1} \cdot \frac{1}{2^n} \cdot (2^n - 1) \\
&= \frac{1}{2^n}
\end{aligned}$$

Now, $\forall x, y \in \{0, 1\}^n$,

$$\begin{aligned}
\Pr[\mathbf{C}_R = y | \mathbf{M}_R = x] &= \Pr[\mathbf{K}_R = \mathsf{K} : y = x \oplus \mathsf{K}] \\
&= \Pr[\mathbf{K}_R = \mathsf{K} : \mathsf{K} = x \oplus y] \\
&= \frac{1}{2^n - 1}
\end{aligned}$$

if x==y, this should be 0, right?

+3 $\therefore$Since $\Pr[\mathbf{C}_R = y | \mathbf{M}_R = x] \neq \Pr[\mathbf{C}_R = y]$, the scheme is not perfectly secure.

B. [Entropy : $4 + (4 \times 2) + (4 \times 2) + (3 + 1) = 24$ points.]

Answers

B.1 We know that,

$$H(\mathbf{K}_R, \mathbf{M}_R, \mathbf{C}_R) = H(\mathbf{K}_R, \mathbf{M}_R) = H(\mathbf{K}_R) + H(\mathbf{M}_R)$$

And, by theorem

$$H(\mathbf{K}_R|\mathbf{C}_R) = H(\mathbf{K}_R) + H(\mathbf{M}_R) - H(\mathbf{C}_R)$$

Using $H(X|Y) = H(X) - H(Y)$,

$$\begin{aligned} H(\mathbf{K}_R|\mathbf{C}_R) - H(\mathbf{M}_R|\mathbf{C}_R) &= H(\mathbf{K}_R) + H(\mathbf{M}_R) - H(\mathbf{C}_R) - H(\mathbf{M}_R|\mathbf{C}_R) \\ &= H(\mathbf{K}_R, \mathbf{M}_R, \mathbf{C}_R) - H(\mathbf{C}_R) - H(\mathbf{M}_R|\mathbf{C}_R) \\ &= H(\mathbf{K}_R, \mathbf{M}_R, \mathbf{C}_R) - H(\mathbf{M}_R, \mathbf{C}_R) \\ &= H(\mathbf{K}_R|\mathbf{M}_R, \mathbf{C}_R) \geq 0 \end{aligned}$$

+4

$\therefore H(\mathbf{K}_R|\mathbf{C}_R) \geq H(\mathbf{M}_R|\mathbf{C}_R)$

B.2 Since messages and keys are equiprobable, $\Pr(\mathbf{M}_R = \mathsf{M}) = \frac{1}{26}\ \forall \mathsf{M} \in \mathbb{Z}_{26}$ and $\Pr(\mathbf{K}_R = \mathsf{K}) = \frac{1}{312}\ \forall \mathsf{K} \in \mathbb{Z}_{26}^* \times \mathbb{Z}_{26})$. So $\Pr(\mathbf{C}_R = \mathsf{C}) = \frac{1}{26}\ \forall \mathsf{C} \in \mathbb{Z}_{26}$.

$$\begin{aligned} H(\mathbf{K}_R) &= \sum_{\mathsf{K} \in \mathbb{Z}_{26}^* \times \mathbb{Z}_{26}} \Pr(\mathbf{K}_R = \mathsf{K}) \cdot \log_2 \frac{1}{\Pr(\mathbf{K}_R = \mathsf{K})} \\ &= \sum_{\mathsf{K} \in \mathbb{Z}_{26}^* \times \mathbb{Z}_{26}} \frac{1}{312} \cdot \log_2 312 \\ &= \log_2 312 \\ &= 8.285 \text{ (approx)} \end{aligned}$$

$$\begin{aligned} H(\mathbf{M}_R) &= \log_2 26 \\ &= 4.7 \text{ (approx)} \end{aligned}$$

$$H(\mathbf{C}_R) = 4.7 \text{ (approx)}$$

$$\begin{aligned} H(\mathbf{K}_R|\mathbf{C}_R) &= H(\mathbf{K}_R) + H(\mathbf{M}_R) - H(\mathbf{C}_R) && \text{(Using Theorem)} \\ &= \log_2 312 = 8.285 \text{ (approx)} \end{aligned}$$

+4 $\therefore H(\mathbf{K}_R|\mathbf{C}_R) = 8.285$

$$\begin{aligned} H(\mathbf{M}_R, \mathbf{C}_R) &= \sum_{\mathsf{C} \in \mathbb{Z}_{26}} \sum_{\mathsf{M} \in \mathbb{Z}_{26}} Pr(\mathbf{C}_R = \mathsf{C}, \mathbf{M}_R = \mathsf{M}) \cdot \log_2 \frac{1}{Pr(\mathbf{C}_R = \mathsf{C}, \mathbf{M}_R = \mathsf{M})} \\ &= \sum_{\mathsf{K} \in \mathbb{Z}_{26}^* \times \mathbb{Z}_{26}} \Pr(\mathbf{K}_R = \mathsf{K}) \cdot \log_2 \frac{1}{\Pr(\mathbf{K}_R = \mathsf{K})} && (\mathsf{C} = E_{\mathsf{K}}(\mathsf{M}) \text{ for some } \mathsf{K} \in \mathbf{K}) \\ &= H(\mathbf{K}_R) \\ &= \log_2 312 \end{aligned}$$

incorrect, this term is 2*log_2(26) [check]

$$\begin{aligned} H(\mathbf{K}_R|\mathbf{M}_R, \mathbf{C}_R) &= H(\mathbf{K}_R, \mathbf{M}_R, \mathbf{C}_R) - H(\mathbf{M}_R, \mathbf{C}_R) \\ &= H(\mathbf{K}_R) + H(\mathbf{M}_R) - H(\mathbf{K}_R) \\ &= \log_2 26 \\ &= 4.7 \text{ (approx)} \end{aligned}$$

+2

the answer is log_2(12)

$\therefore H(\mathbf{K}_R|\mathbf{M}_R, \mathbf{C}_R) = 4.7$

B.3 • $f(x) = 7^x$

$$H(\mathbf{R}) = \sum_{\mathsf{R} \in R} \Pr(\mathbf{R} = \mathsf{R}) \cdot \log_2 \frac{1}{\Pr(\mathbf{R} = \mathsf{R})}$$

this is an equality as 7^x is bijection

$$\geq \sum_{x \in D} \Pr(\mathbf{R} = 7^x) \cdot \log_2 \frac{1}{\Pr(\mathbf{R} = 7^x)} \qquad (f(D) \subseteq R)$$

$$= \sum_{x \in D} \Pr(\mathbf{D} = x) \cdot \log_2 \frac{1}{\Pr(\mathbf{D} = x)}$$

$$= H(\mathbf{D})$$

0

$\therefore H(\mathbf{R}) \geq H(\mathbf{D})$

B.4 Let $\min_{z \in Z} \log_2 \frac{1}{\Pr(\mathbf{Z}=z)} = k$

$$H(\mathbf{Z}) = \sum_{z \in Z} \Pr(\mathbf{Z} = z) \cdot \log_2 \frac{1}{\Pr(\mathbf{Z} = z)}$$

$$\geq \sum_{z \in Z} \Pr(\mathbf{Z} = z) \cdot k \qquad \left(\log_2 \frac{1}{\Pr(\mathbf{Z} = z)} \geq \min_{z_1 \in Z} \log_2 \frac{1}{\Pr(\mathbf{Z} = z_1)} \forall z \in Z\right)$$

$$= k \cdot \sum_{z \in Z} \Pr(\mathbf{Z} = z)$$

$$= k = \min_{z \in Z} \log_2 \frac{1}{\Pr(\mathbf{Z} = z)}$$

$$= -\log_2 \left(\max_{z \in Z} \Pr(\mathbf{Z} = z)\right) = H_\infty(\mathbf{Z})$$

$\therefore H(\mathbf{Z}) \geq H_\infty(\mathbf{Z}) \geq 0$

$H(\mathbf{Z}) = H_\infty(\mathbf{Z})$ when $-\log_2 \left(\max_{z \in Z} \Pr(\mathbf{Z} = z)\right) = -\log_2 (\Pr(\mathbf{Z} = z_1)) \, \forall z_1 \in Z$

$\Rightarrow \max_{z \in Z} \Pr(\mathbf{Z} = z) = \Pr(\mathbf{Z} = z_1) \forall z_1 \in Z$

4

$\therefore$ If $\mathbf{Z}$ has a uniform distribution, $H(\mathbf{Z}) = H_\infty(\mathbf{Z})$.