National Taiwan Normal University
CSIE Information Security

Instructor: Po-Wen Chi
Due Date: March 22, 2021, PM 11:59

Assignment 1

Policies:

- Zero tolerance for late submission.
- Please pack all your submissions in one zip file. **RAR is not allowed!!**
- I only accept **PDF**. MS Word is not allowed.
- Hand-writing is not allowed.
- Please use **Chinese.**

1.1 Entropy of English (10 pts)

You all know that there are 26 letters in English, right? Please calculate the entropy of an English letter in the following two cases.

1. Suppose that all characters are equally likely.
2. Some characters occur much more frequently than others, as shown in table 1.1.

letter	frequency	letter	frequency	letter	frequency	letter	frequency
a	0.08167	b	0.01492	c	0.02782	d	0.04253
e	0.12702	f	0.02228	g	0.02015	h	0.06094
i	0.06966	j	0.00153	k	0.00772	l	0.04025
m	0.02406	n	0.06749	o	0.07507	p	0.01929
q	0.00095	r	0.05987	s	0.06327	t	0.09056
u	0.02758	v	0.00978	w	0.02360	x	0.00150
y	0.01974	z	0.00074				

TABLE 1.1: Letter frequency.

3. Please construct a Huffman code for the English letters based on table 1.1 and calculate the expected value of the symbol length.

For your reference, estimates by Shannon based on human experiments have yielded values as low as 0.6 to 1.3 bits per symbol.

1.2 Secure Pseudo Random Number Generator (10 pts)

Let $G : \{0,1\}^s \to \{0,1\}^n$ be a secure pseudo random number generator, which implies unpredictability. Which of the following is a secure PRG. Please give your reasons.

1. $G'(k) = G(1)$.
2. $G'(k) = G(k)||G(k)$.
3. $G'(k) = G(k)||0$.
4. $G'(k) = G(k) \oplus 1^n$.
5. $G'(k) = G(k \oplus 1^s)$.
6. $G'(k_1, k_2) = G(k_2)||G(k_1)$.

Here $||$ implies concatenation.

1.3 Mutual Information (10 pts)

Definition 1.1 (Mutual Information)**.** Consider two random variables X and Y with a joint probability mass function $p(x, y)$ and marginal probability mass functions $p(x)$ and $p(y)$. The mutual information is the relative entropy between the joint distribution and the product distribution $p(x)p(y)$,

$$I(X;Y) = \sum_{x \in X} \sum_{y \in Y} p(x,y) \log \frac{p(x,y)}{p(x)p(y)}.$$

Please prove

1. $$I(X;Y) = H(X) - H(X|Y).$$
2. $$I(X;X) = H(X).$$

1.4 Perfect Secrecy (15 pts)

Let $M = K = C = \{0, 1, 2, \ldots, 255\}$. Given the following encryption scheme,

- $\mathbf{Enc}(m, k) = m + k \pmod{256}$.

- $\mathbf{Dec}(c, k) = c - k \pmod{256}$.

Does this cipher have perfect secrecy? Why?

1.5 A Broken One-Time Pad (15 pts)

Consider a variant of the one time pad with message space $\{0,1\}^L$ where the key space is restricted to all L-bit strings with an even number of 1's. Give an efficient adversary whose semantic security advantage is 1.

1.6 Programming: Never Use One Time Pad Twice (20 pts)

In this class, I told you that you cannot use the same key twice in the one time pad cipher. Now let's see what happens if you use this twice. I will give you ten ciphertexts encrypted through the same key. The key size is larger than all messages. Then, I will give you another challenge ciphertext encrypted by the same key. Please decrypt the challenge ciphertext for me.

Hint: What will happen if you XOR a space with a character [a-zA-Z]?

- Ciphertexts:

  1. 68 C0 21 F4 F1 0A 75 6C 1F E3 87 FE 44 F8 D6 EA
     55 E2 56 1B 4C D3 78 03 49 BD FF 70 10 A6 19 44
     86 E1 19 AC 3F 26 7C 88 D8 C7 BF 06 5B B0 B8 4B
     31 A7 DF A7 4F E8 74 21 01 9A 04 F9 0E B1 F4 1B
     FF A3 C5 E0 B5 94 B4 FF 8F FF 5C DE 63 23 65 38
     5C 80 C0 1C 4D FC 5D 32 DF 1C 17 67 0F EE 87 05
     2F 08 EB 4E F0 61 38 3A 43 71 09
  2. 74 DA 6D F8 F1 59 21 7D 15 B6 C5 ED 57 F4 98 A1
     1A F9 5A 5E 0D CB 31 10 48 B4 E9 23 1E BA 1F 11
     86 EB 08 E0 3A 26 7C 89 D9 93 E8 03 47 B0 B8 4B
     2B BA DF A7 40 F8 6E 3B 46 C8 00 B5 13 FA A0 31
     F2 B2 8C FB A5 C9
  3. 74 D3 6D E4 A2 4B 72 24 09 AA 8B A0 05 F3 CD B2
     55 E5 56 1B 4C D2 70 1C 58 A2 BA 38 12 A6 0B 58
     CA E4 5C A6 36 39 28 C9 96 BE A7 1B 12 B2 B7 19
     3B AC 85
  4. 63 D1 62 FC F7 59 64 24 33 E3 84 E1 05 D9 DD B4
     16 E3 52 1B 4C EF 7E 1E 4F BE EE 71 57 9D 58 59
     C9 A2 12 AF 27 75 32 82 D3 83 E8 1A 5D F3 B2 0E
     7E BD D5 EB 46 B3

5. 76 D1 21 FE E3 44 6F 6B 0E E3 86 ED 51 F2 D0 E6
   14 B6 4A 0C 0D D6 7F 57 58 B0 E8 3C 1E B1 0A 1D
   D2 EA 1D AE 73 21 34 82 96 93 A1 03 57 F3 A4 03
   3F BD 9A EE 56 BD 6B 30 40 9E 04 E6 5B BF B5 3A
   F5 E6 91 E2 E0 95 B5 B6 92 BA 56 DB 26 70 7E 7D
   1F 98 DD 1D 51 F1 0E 65 C1 01 13 62 41 AD C5 1F
   60 1E AE 19 ED 7D 35 75 5A 60 46 DF BF E2 AC E5
   13 CE 49 C4 8A 85 A7 E8 10 2E 7D 3A 63 7B 7F 6D
   3F 6D 3F 65 A4 D7 BE 77 31 9E 59 6E 14

6. 76 DC 64 EF E7 5C 64 76 5A B7 8D E9 57 F4 98 AF
   06 B6 56 0B 01 DE 7F 57 53 B0 EE 25 05 B1 54 1D
   D2 EA 19 B2 36 75 35 94 96 83 BA 0F 5F B2 FE

7. 75 DC 64 BD EB 47 71 6B 09 B0 8C EE 49 F4 98 A5
   1A E3 52 1A 4C D1 7E 03 1D B9 FB 26 12 F4 10 5C
   D6 F2 19 AE 36 31 70 C7 C2 8F AD 1C 57 B5 BF 19
   3B E9 CE EF 47 BD 6E 38 51 87 12 E6 1E FD B8 31
   B1 AB 90 FE B4 C7 A2 BA DC EA 56 C6 30 3E 6F 31
   19 D4 DB 07 19 E7 0D 2C C2 0D 5F 61 07 E3 CB 1B
   30 19 AA 4B F8 7B 33 30 45 2B

8. 55 DC 64 BD EF 45 73 61 5A B4 80 AC 49 F4 D9 B4
   1B BA 1E 0A 04 DA 31 1B 58 A2 E9 70 16 BA 1C 1D
   CA E7 0F B3 73 38 33 93 DF 91 AD 4E 45 B6 F0 0D
   37 A7 DE A7 44 F2 75 75 52 9D 08 F6 1E FB B1 6B
   B1 84 90 F9 E0 81 AF AD DC F7 4C C7 27 32 7F 71
   5C 83 D7 49 5B F1 1A 2C D8 48 0B 61 41 AB CB 1D
   25 5C AA 19 EA 60 22 25 44 6C 54 C5 A5 A5 E4 E3
   10 D2 43 D4 85 D1 A7 E9 5E 7E 60 39 35 73 7E 6D
   3F 75 3D 36 E4

9. 60 DA 21 FC F0 49 69 65 1F AC 89 E3 42 F8 CB B2
   55 FF 4D 5E 18 D7 74 57 5F B4 E9 24 57 BC 0D 4E
   C4 E3 12 A4 73 34 7C 90 D9 8A A9 00 12 B0 B1 05
   7E A1 DB F1 47 B3 27 01 49 8D 41 FA 1B FB B1 26
   B1 B5 8D E8 E0 80 A5 AB 8F BA 4D DD 26 77 60 32
   0E 91 92 00 57 E0 18 37 D3 1B 0B 6B 05 E3 C2 0E
   60 15 B8 19 F0 7B 70 3D 53 77 09

10. 75 DC 64 BD F6 58 74 70 12 EF C5 E4 4A E6 DD B0
    10 E4 1E 0B 0B D3 68 57 54 BF BA 39 03 A7 1D 51
    C0 AE 5C A9 20 75 3D 8B C1 86 B1 1D 12 B0 A5 19
    37 A6 CF F4 02 FC 69 31 01 8A 04 F4 02 EB BD 32
    E4 AA C5 F9 AF C7 B3 BA 99 F1 5C C7 30 77 6C 3B
    08 91 C0 49 50 E0 53

- Challenge Ciphertext:
  - 68 DA 21 FE ED 44 77 61 08 B0 84 F8 4C FE D6 EA
    55 E6 51 17 02 CB 62 57 5C A3 F3 23 12 F5 58 74
    C0 A2 1D E0 3B 20 31 86 D8 C7 AA 0B 5B BD B7 4B
    3D A6 D4 F1 47 EF 74 30 52 C8 0C E0 14 F7 F8 74
    F8 B2 C5 E4 B3 C7 A9 B2 8C F5 4A C6 2A 35 61 38
    5C 92 DD 1B 19 FC 14 28 96 1C 10 2E 00 B5 C5 02
    24 5C BF 51 FC 35 24 27 43 71 4F 8D

1.7 WEP Cracker (20 pts)

In this class, I have told you that WEP is not a secure wireless encryption method. Now it is your turn to check this yourself. I will set up a wireless AP on PC room. Please try to get its WEP password.

- SSID: NTNU_IS_2021

You can google how to do this, but remember that you need to know what you are doing. Describe your approach in detail. Do not just write down the steps or commands without any explanation.