National Taiwan Normal University
CSIE Information Security

Instructor: Po-Wen Chi
Due Date: March 17, 2024, 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 Joint entropy (10 pts)

Please prove

1. $$H(X,Y) = H(Y) + H(X|Y)$$
2. $$H(X,Y) \leq H(X) + H(Y)$$

1.2 Encryption Chain (10 pts)

Let $\mathcal{E} = (E, D)$ be a cipher defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ where $\mathcal{K} = \mathcal{M}$. Let $\mathcal{E}' = (E', D')$ be a cipher where encryption is defined as

$$E'((k_1, k_2), m) := (E(k1, k2), E(k2, m)) \in \mathcal{C}^2.$$

Show that if $\mathcal{E}$ is perfectly secure then so is $\mathcal{E}'$.

1.3 Semantic Security (20 pts)

Let $\mathcal{E} = (E, D)$ be a semantically secure cipher defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ where $\mathcal{M} = \mathcal{C} = \{0,1\}^L$. Which of the following encryption algorithms yields a semantically secure scheme? Either give an attack or provide a security proof via an explicit reduction.

- $E_1(k, m) := 0||E(k, m)$
- $E_2(k, m) := E(k, m)||\text{Parity}(m)$
- $E_3(k, m) := \text{reverse}(E(k, m))$
- $E_4(k, m) := E(k, \text{reverse}(m))$

1.4 Malleability (10 pts)

Suppose you are told that the stream cipher encryption of the message "I love cryptography." is **49913FF7731C1E74510611018BE35110495CCAA7** (the plaintext letters are encoded as 8-bit ASCII and the given ciphertext is written in hex). What would be the stream cipher encryption of the message "I hate cryptography." under the same key?

1.5 Slide Attack (10 pts)

In this class, I have told you that a mandatory requirement of a Feistel network encryption is that the key in each round must be independent. If not, there will be an attack called slide attack.

So what is a slide attack? Please read the reference paper and describe it in your own words.

https://link.springer.com/content/pdf/10.1007/3-540-48519-8_18.pdf

1.6 Programming: Never Use One Time Pad Twice (10 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. 36 00 BE F7 B0 67 6D 04 CA 57 EB 32 D5 66 AF EB
     22 86 76 B3 60 61 B9 8F 5D E6 9E 3E D1 CD 03 E5
     89 D9 CE C6 CD E4 1D 0F E1 32 44 47 39 77 1E 78
     71 F6 2B 5A 33 E9 14

2. 23 48 AC B8 AA 6E 68 50 9E 56 F9 66 9D 7B AF E4
   2D D4 05 B3 7E 67 AF CF 5D D0 98 3F 83 DC 4B E0
   8E D8 D8 C6 C5 E5 58 41 E0 29 10 12 30 73 1E 78
   72 F8 7C 6B 37 E0 1A 30 A4 6B 8A 4A 4B 8A DB E0
   B9 0D 73 56 C2 15 F6
3. 35 00 A2 F7 9F 6D 68 4F CA 69 F0 6B 9A 7C E7 EB
   3F 86 43 B3 6A 63 E9 C1 2A EF 89 7A 82 CC 08 E4
   C7 DC D8 87 D9 E2 01 0F E6 33 10 13 36 71 04 36
   66 BA 3D 5C 3A BA
4. 3B 07 AE F7 B9 70 69 50 99 4B F6 7E D3 6F E7 F6
   6C C7 4B B6 29 4F F6 8C 12 E8 9E 76 D1 D3 04 E5
   89 DB D9 C6 CE EF 58 5B E7 38 10 00 31 7C 04 36
   79 B0 7C 59 30 F7 4E 28 A5 78
5. 2B 1C FC A4 F8 75 64 11 9E 1E F9 7E D6 28 FB EA
   29 86 42 BB 7B 6A A5 C1 0E EE 9E 3D D1 D8 1F AC
   90 DB D9 82 C5 F8 1F 5C A1 7D 64 0F 3B 61 57 72
   7F B2 32 18 2B A5 51 33 A4 6A C3 58 03 82 C1 E0
   B1 18 20 5E 8B 0F FD 4A FD 9F C2 8D CF
6. 2D 1D A9 F7 B4 6B 7A 15 99 1E EF 7B D6 64 AF E1
   24 C7 4B B5 6C 26 A1 89 18 E9 D0 2E 9E D4 04 FE
   95 D1 CA C6 CF F9 15 4A FC 73 10 33 31 76 1E 71
   7E A2 7C 50 2A F7 1A 35 AE 7C 91 5B 18 C3 D1 B2
   BB 03 3D 1B DF 13 F7 4A EA 9F DF 9E 80 47 93 C0
   6C 46 E4 95 81 84
7. 23 48 A8 B8 B6 65 2C 00 86 5F E1 77 DE 28 E0 EC
   6C C7 05 A1 66 6A B9 C1 0E E6 88 35 81 D1 04 E2
   82 90 9D A7 8C F5 0A 4E F5 24 10 14 31 6D 19 72
   38 F6 1D 1F 33 EA 54 38 A7 64 C3 5C 04 96 DB A4
   FA 54 12 1B C8 09 EB 4A FA 9E CD 9E C1 5D 82 8C
   64 47 B1 8D 81 8A 94 4C 71 BD 6F 8C A0 CF F8 06
   1A 23 93 F7 A4 23 A9 BF 91
8. 31 07 FB A4 AC 63 75 50 9D 57 EC 7A 9A 65 EA A2
   2D C8 41 F2 61 69 BA 85 5D EA 95 7A 85 D0 0C E4
   93 9E DC 88 C8 B6 1C 4E E1 3E 55 47 32 71 1C 73
   36 BF 28 4C 7F F1 52 38 EB 71 82 5C 1F C3 DB A9
   B3 1C 27 1B C4 1D B2 1E E6 93 8C 9D 8E 5B 8B 84
   26
9. 3B 0D A8 FB F8 71 78 19 86 52 B4 32 F3 28 FC F6
   25 CA 49 F2 6B 63 BA 88 18 F1 95 74 D1 F0 4B E7
   89 D1 CA C6 CD E5 58 43 E0 33 57 47 3F 6B 57 5F
   36 B5 3D 51 7F EE 5F 38 BB 3D 81 4A 07 8A D0 B6
   BD 1A 34 17 8B 32 B5 06 E2 D6 C0 83 97 4C C9

10. 31 09 B2 B0 B7 6C 2C 07 8B 4D B8 71 C8 69 F5 E7
    28 8A 05 B0 7C 72 F6 92 15 E2 D0 2D 90 CA 4B FE
    82 DF D1 C6 CD F8 1C 0F E9 32 42 47 31 76 12 36
    7B B9 31 5A 31 F1 16 7D 82 3D 80 40 1E 8F D1 E0
    B2 11 36 57

- Challenge Ciphertext:
  - 2C 07 AF F7 B7 6C 60 09 CA 5A F7 77 C9 28 C8 ED
    28 86 55 BE 68 7F F6 85 14 E4 95 76 D1 DB 1E F8
    C7 D6 D8 C6 DF F9 15 4A FB 34 5D 02 2D 38 03 7E
    64 B9 2B 4C 7F F1 52 38 A6 3D 94 47 0E 91 D0 E0
    A0 1C 36 42 8B 18 F3 04 E0 99 D8 CA 83 4C C7 93
    6D 51 FF D6

1.7 Lab: Pseudo Random Number Generator (15 pts)

In this class, I have told you that there is no real pseudo random number generator (PRG). However, PRG is very important to us. How does a system generate a random number? This lab will guide you to see how your system works.

- Lab: https://seedsecuritylabs.org/Labs_20.04/Crypto/Crypto_Random_Number/

You need to submit a detailed lab report, with screenshots, to describe what you have done and what you have observed. You also need to provide explanation to the observations that are interesting or surprising. Please also list the important code snippets followed by explanation. Simply attaching code without any explanation will not receive credits.

1.8 Lab: Test Suite for Random Numbers (15 pts)

I assume that you have completed the previous lab. NIST actually provides a test suite for random numbers. Please download the tool and use this tool to compare the evaluation result between standard C random(), /dev/random and /dev/urandom.
https://csrc.nist.gov/projects/random-bit-generation/documentation-and-softw