2018 Spring

Information Security Midterm

Time: 2018/04/24 PM 2:20 ~ PM 5:20

Student ID:

Name:

This is a closed-book exam. Cheating is definitely not allowed not allowed. Note that the total points are 30 **+ 2** instead of 100.

1. Let $\mathcal{P}$, $\mathcal{C}$, $\mathcal{K}$ be the message space, ciphertext space and key space respectively of an encryption scheme. Let H($\mathcal{X}$) be the entropy of a random variable $\mathcal{X}$ defined as follows:

$$H(X) =- \sum_{i=1}^{n} p_i log\ p_i$$

Please answer the following questions.

1.1. Why H($\mathcal{P}$ | $\mathcal{C}$, $\mathcal{K}$) = 0? (1 pt)

Given the ciphertext and the key, you know the plaintext since it is the decryption of the given ciphertext under the given key.

1.2. Why H($\mathcal{C}$ | $\mathcal{P}$, $\mathcal{K}$) = 0? (1 pt)

Given the plaintext and the key, you know the ciphertext since it is the encryption of the given plaintext under the given key

1.3. Please prove that H($\mathcal{P}$) + H($\mathcal{K}$) = H($\mathcal{C}$, $\mathcal{K}$) (1 pt)

H($\mathcal{P}$, $\mathcal{K}$, $\mathcal{C}$) = H($\mathcal{P}$, $\mathcal{K}$) + H($\mathcal{C}$ | $\mathcal{P}$, $\mathcal{K}$) = H($\mathcal{P}$, $\mathcal{K}$) = H($\mathcal{P}$) + H($\mathcal{K}$)
H($\mathcal{K}$, $\mathcal{C}$, $\mathcal{P}$) = H($\mathcal{C}$, $\mathcal{K}$) + H($\mathcal{P}$ | $\mathcal{C}$, $\mathcal{K}$) = H($\mathcal{C}$, $\mathcal{K}$)

2. Let $G(k) : \{0,1\}^s \rightarrow \{0,1\}^n$ be a secure PRF (pseudo random function). Please determine if the following is also a secure PRF. Note that || means concatenation.

2.1. G'(k) = G(k) || G(k) (1 pt) False

2.2. G'(k_1, k_2) = G(k_1) || G(k_2) (1 pt) True

2.3. G'(k) = G(k) || 0 (1 pt) False

2.4. G'(k) = G(k) ⊕ 1^n (1 pt) True

2.5. G'(k) = G(k⊕ 1^n) (1 pt) True

3. Let X be a uniform random variable over the set $\{0,1\}^n$. Let Y be an arbitrary random variable over the set $\{0,1\}^n$ (not necessarily uniform). Define the random variable Z=X⊕Y. What is the probability that Z=0^n and Why? (2 pt)

$1/2^n$.

Observe that whatever Y is, the probability that Z=0 equals to X=Y.

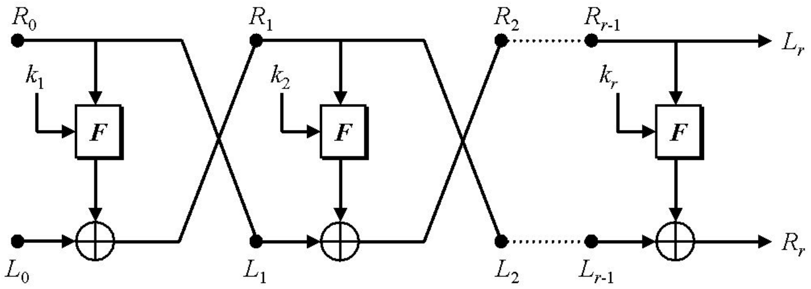
Since X is uniform, the probability will be $1/2^n$.

4. Please calculate modular multiplicative inverses of given integers and modulos.

4.1. 50 mod 71 (1 pt) 27

4.2. 43 mod 64 (1 pt) 3

5. In this class, I have introduced Feistel Network Structure as follows:



Please show that one round and two rounds Feistel Network are not secure at all. (2 pt)

One round: L_1 will be R_0 which will be plaintext.
Two round: $L_2 = R_1 = L_0 \oplus F(k_1, R_0)$. So we can have $L_2 \oplus T = R_1 \oplus T = L_0 \oplus F(k_1, R_0) \oplus T$ and can break the game.

6. DES is an encryption where the key size is 56 bits. Why double DES cannot enhance the key size to 112 bits? Please explain it by your word and not just write one phrase. (2 pt)

Meet in the middle attack.

7. What is semantic secure? Please write down its definition. And please show that a stream cipher is semantic secure and the attacker advantage is bounded by 2* Adv_{PRG}. (2 pt)

Please see the lecture slide.

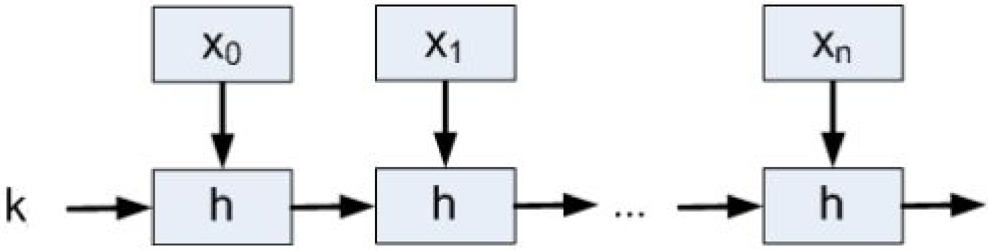
8. In RSA, we need to generate two distinct primes p, q and then calculate N=pq as the modulus. Now there is someone who only generates one prime p and use p as the modulus. Please show the resulting scheme will be easily broken. (2 pt)

Given e as the public key.
Since ϕ(p) = p - 1, it is easy for everyone to get d by calculating e’s multiplicative inverse modulo p-1.

9. What is Diffie–Hellman key exchange protocol? Please show one vulnerability of this key exchange protocol. Again, do not write phrase only. Please explain how it works. (2 pt)

Alice generates a random number a.
Alice → Bob: g^a
Bob generates a random number b.
Bob → Alice: g^b
The key will be g^{ab}.
Man in the middle attack.

10. Someone designs a MAC scheme which works as follows:



h is a secure PRP (Pseudo Random Permutation) function. Please explain why this MAC scheme is not secure. (2 pt)

Cascade problem.

11. What is TCP SYN FLOOD Attack? Please describe how it works. (2pt)

A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.

The malicious client can either simply not send the expected ACK. The server will wait for the acknowledgement for some time. In an attack, the half-open connections created by the malicious client bind resources on the server and may eventually exceed the resources available on the server.

12. ElGamal is a public key encryption scheme that works as follows:

Key Setup:

Generate a cyclic group of order q with a generator g.

Select a random number x ← {0, …, q-1}

Public key will be g^x,G,q

Private key will be x.

Encryption:

Given a message m where m is in G.

Select a random number y ← {0, …, q-1}

The ciphertext will be $g^y, c=m\cdot g^{xy}$

Please show that given $g^y, m\cdot g^{xy}$, you can generate a valid ciphertext that is encrypted by 3m. (2pts)

c’=3*c

13. A replay attack is a network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. For example, Alice encrypted her password and send to the server for authorization. If Eve catches the packets, she can also send the packet to the server and also be authorized. Please provide an approach to defend this attack. (2pts)

Timestamp.

11. (Bonus) What do RTFM and STFG mean? If you do not like the third letter, you can skip it. (1 pts)

RTFM = Read the fucking manual.
STFG = Search the fucking Google.

12. (Bonus) Do you have suggestions about this course? Please provide some points that I can improve in the following class. (1pts)