جامعة بيرزيت
BIRZEIT UNIVERSITY

Faculty of Engineering and Technology
Electrical and Computer Engineering Department

ENCS4320, Applied Cryptography

Midterm Exam (V1)

Wednesday, 3/01/2023

Name:__________________________________**ID**:__________________________

1. (**2 pts**) When using one-time pad cipher, why must we not use the same key a second time?

Recall that a message m is encrypted as $c = m \oplus k$ Using the same key twice, we can combine the ciphertexts $c_1 = m_1 \oplus k$ and $c_2 = m_2 \oplus k$ to obtain

$$c_1 \oplus c_2 = m_1 \oplus m_2$$

This is information about the plaintexts! (In fact, if the plaintexts are text encoded in ASCII this is usually enough to obtain both m_1 and m_2 from $m_1 \oplus m_2$.)

2. (**2 pts**) The design of a block cipher is almost an art, but there are two guiding principles due to Claude Shannon, the father of information theory. What are these two principles? Briefly explain what they refer to.

The two principles are confusion and diffusion.

Confusion refers to making the relationship between the ciphertext and the key as complex and involved as possible (for instance, changing one bit of the key should change the ciphertext completely).

Diffusion refers to dissipating the statistical structure of the plaintext over the bulk of the ciphertext (for instance, changing one bit of the plaintext should change the ciphertext completely; likewise, changing one bit of the ciphertext should change the plaintext completely).

3. (**4 pts**) For the following encryption scheme, state whether the scheme is perfectly secret. Justify your answer.

The message space is $\mathcal{M} = \{0, \dots, 4\}$. Algorithm Gen chooses a uniform key from the key space $\{0, \dots, 5\}$.

$$\mathrm{Enc}_k(m) = (k + m) \bmod 5,$$

and

$$\mathrm{Dec}_k(c) = (c - k) \bmod 5.$$

The scheme is not perfectly secret. To see this, we can use the equivalent definition of perfect secrecy. Formally, for every $m, m' \in \mathcal{M}$ and every $c \in \mathcal{C}$, $\Pr[\mathrm{Enc}_k(m) = c] = \Pr[\mathrm{Enc}_k(m') = c]$. If the message is 0, then the ciphertext is 0 if and only if $k \in \{0, 5\}$. So $[Enc_k(0) = 0] = \frac{2}{6} = 1/3$.

On the other hand, if the message is 1, then the ciphertext is 0 if and only if $k = 4$. So

$$\Pr[\mathrm{Enc}_k(m = 0) = 0] = 2/6 \neq \Pr[\mathrm{Enc}_k(m = 1) = 1/6]$$

$m = 0$	$m = 1$
$(0 + 0) \bmod 5 = 0$	$(1 + 0) \bmod 5 = 1$
$(0 + 1) \bmod 5 = 1$	$(1 + 1) \bmod 5 = 2$
$(0 + 2) \bmod 5 = 2$	$(1 + 2) \bmod 5 = 3$
$(0 + 3) \bmod 5 = 3$	$(1 + 3) \bmod 5 = 4$
$(0 + 4) \bmod 5 = 4$	$(1 + 4) \bmod 5 = 0$
$(0 + 5) \bmod 5 = 0$	$(1 + 5) \bmod 5 = 1$

4. (**4 pts**) Consider a block cipher with 5-bit block size and 5-bit key size such that

$$E_k(b_1 b_2 b_3 b_4 b_5) = (b_1 b_2 b_3 b_4 b_5) \oplus k$$

Encrypt $m = (010101010101010)_2$ using k=$(10001)_2$ and **ECB** mode.

$m = m_1 m_2 m_3$ with $m_1 = 01010, m_2 = 10101, m_3 = 01010$.

$$c_1 = E_k(m_1) = 01010 \oplus 10001 = \mathbf{11011}$$

$$c_2 = E_k(m_2) = 10101 \oplus 10001 = \mathbf{00100}$$

Since $m_3 = m_1$, we have $c_3 = c_1$.

Hence, the ciphertext is $c = c_1 c_2 c_3 = (\mathbf{110110010011011})$.

5. (**2 pts**) What is the effect of a single-bit error in the ciphertext when using the CTR-mode of operation?

Say a message $m_1, m_2, \ldots$ is encrypted to give a ciphertext $c_0, c_1, c_2, \ldots$, and then a single bit is flipped somewhere in the ciphertext. We look at the effect of decrypting the resulting (modified) ciphertext using each of the stated modes to obtain a message $m_1', m_2', \ldots$

CTR mode. A bit flip in c_i for $i > 0$ only causes a bit flip in message block m_i.

However, a bit flip in c_0 will (in general) result in all the plaintext blocks being recovered incorrectly.

6. (**3 pts**) Say CBC-mode encryption is used with a block cipher having a 256-bit key and 128-bit block length to encrypt a 1024-bit message. What is the length of the resulting ciphertext in bits?

The message is 8 = 1024/128 blocks long.

The ciphertext (which includes an IV) is 9 blocks long.

Thus, the ciphertext is 1152 bits long.

7. (**5 pts**) Let F be a PRP block cipher with 256-bit block length. Consider the following encryption scheme for 512-bit messages: to encrypt message $M = m_1 \parallel m_2$ using key k =128-bit (where $|m_1| = |m_2| = 256$, choose random 256-bit r and compute the ciphertext $r \parallel F_k(r) \oplus m_1 \parallel m_2$. Is this encryption scheme CPA-secure or not? Explain your answer.

Let m_1 and m_2 be arbitrary but distinct.

Using the encryption oracle, obtain an encryption $r \| c_1 \| c_2$ of $m_1 \| m_2$.

Output messages $M_0 = m_1 \| m_2$ and $M_1 = m_2 \| m_1$.

Not that the last block is not encrypted. Therefore,

if $c_2 = m_2$ → the challenge cipher for M_0

if $c_2 = m_1$ → the challenge cipher for M_1

The attacker win the game with probability 1.

8. (**4 pts**) Assume F be a PRF where the key space $\mathcal{K} = \{0,1\}^n$ and message $M = m_1 \parallel \cdots \parallel m_\ell$ with $m_i \in \{0,1\}^n$ for $i \in [1, \ell]$. The MAC scheme generates the tag $t = F_k(m_1) \oplus \ldots \oplus F_k(m_\ell)$. Is this MAC construction of is secure or insecure? Explain your answer.

This is **insecure** MAC.

If *t* is the tag for $m_1 \| m_2 \| \cdots \| m_l$, *t* would be a valid forgery for $m_2 \| m_1 \| m_3 \| \cdots \| m_l$ since changing the order of message blocks does not change the value of the tag given by $F_k(m_1) \oplus \cdots \oplus F_k(m_l)$.

9. If you need to build an application that needs to encrypt multiple messages using a single key, what encryption method should you use? Implement Encrypt-and-MAC or Use a standard implementation of one of the authenticated encryption modes, such as GCM. Explain your answer.

Use a standard implementation of one of the authenticated encryption modes, such as GCM.
Normally, you should use two different keys if you use Encrypt-and-MAC yourself

10. (**4 pts**) Consider a cryptographic hash function $h(x)$ with n-bit digest.

(a) What does mean for a hash function $h(x)$ to be one-way?

(b) What does mean for hash function $h(x)$ to be (strongly) collision-resistant?

(a) $h(x)$ is called one-way if, given y, it is computationally infeasible to compute m such that $h(m) = y$.

Such a function is also called preimage-resistant.

(b) $h(x)$ is called (strongly) collision-resistant if it is computationally infeasible to find two messages m_1, m_2 such that $h(m_1) = h(m_2)$.