# Internet Infrastructure Security (COMP444)
# Assignment One

Each question carries six marks, unless stated otherwise.
** Due on 7 March 2014 **

Rocky K. C. Chang

March 13, 2014

1. `[6 marks]` (Shift cipher) Consider the Shift cipher in slide 10 of Introduction to Classical Cryptosystems (i.e., $\mathbf{M} = \mathbf{C} = \mathbf{K} = \{0, 1, 2, \cdots, 25\}$). If we use $K = \{0, 1, \cdots, 50\}$ instead, answer the following questions.

   (a) `[3 marks]` Is the resulting cryptosystem still legitimate?

   (b) `[3 marks]` Does the larger key space increase the security of the cryptosystem?

2. `[6 marks]` (A stream cipher) A stream cipher generates a key stream and encrypts a message by exclusive-ORing it with the key stream. The receiver side also generates the same key stream to decrypt the message by performing exclusive-OR.

   Consider the following stream cipher. The key stream is given by $k_0, k_1, k_2, \cdots$. The values of $k_0$ is initialized by an IV, whereas other $k_i$s are generated by an encryption function $E()$.

$$\begin{aligned} k_0 &= IV \\ k_i &= E(k, k_{i-1}),\ for\ i \geq 1 \\ c_i &= p_i \oplus k_i \end{aligned}$$

   One major problem with this cipher is that two different messages using the same IV will have the same key stream. Consider that two different plaintexts $P$ and $P'$ are encrypted by the same key stream and they produce ciphertexts $C$ and $C'$, respectively.

   (a) `[4 marks]` What kind of information does they leak out to an attacker?

   (b) `[2 marks]` If the attacker also knows $P$ or $P'$, what else will he know and why?

3. `[6 marks]` (A different CBC) Consider a slightly different CBC encryption in Figure 1.

   (a) `[3 marks]` Based on Figure 1, write down the encryption and decryption functions using our usual notations $m_i$ and $c_i$ for the $i$th plaintext block and $i$th ciphertext block, respectively.

   (b) `[3 marks]` If bit 3 of $c_i$ is modified, what kind of changes will be made to the plaintext after decryption? (Hint: slide 37 of Introduction to Block Ciphers)

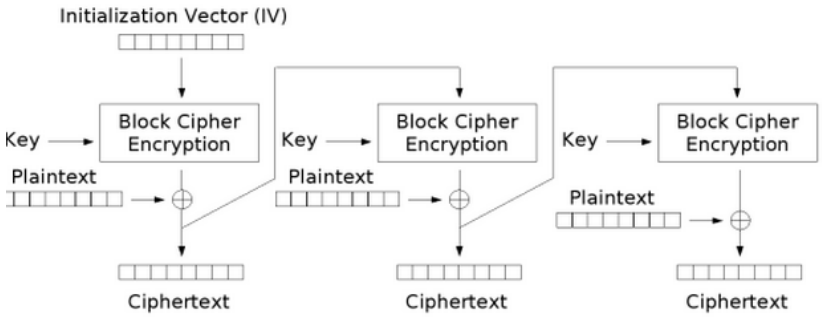


Figure 1: Encryption using a slightly different CBC.

4. `[10 marks]` (CBC ciphertext stealing) CBC ciphertext stealing is a method to handle a block cipher's requirement on the size of the plaintext without padding (as you have seen from the Padding Oracle attack, allowing padding could breach security).

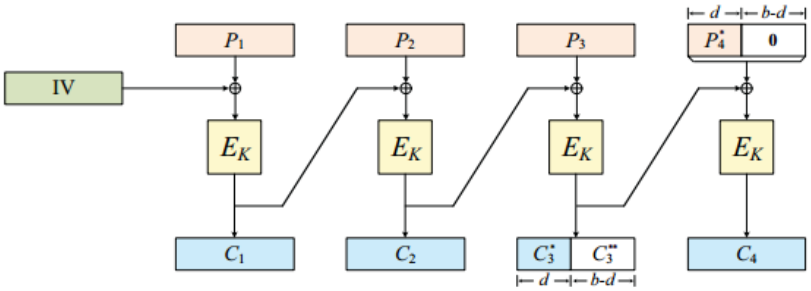


Figure 2: CBC ciphertext stealing.

Figure 2 illustrates the method. The size of the last plaintext "block" ($P_4^*$) is less than a block size (in $b$ bits). In particular, $P_4^*$ has $d$ bits. It is padded with $\mathbf{0}$ ($b-d$ 0s) and then goes to the last stage of encryption. Note that the third ciphertext block consists of two parts: $C_3^*$ (in $d$ bits) and $C_3^{**}$ (in $b-d$ bits). Note that the second part, which is distinguished by white color, is not sent out. The encrypting node then sends out $C_1$, $C_2$, $C_4$, and $C_3^*$. Answer the following questions about this method after a decrypting node receives the ciphertext.

(a) `[6 marks]` Show that the decrypting node can obtain $P_4^*$ by taking the first $d$ bits from $D_K(C_4) \oplus (C_3^* \,||\, \mathbf{0})$, where $D_K()$ is the corresponding decryption function.

(b) `[4 marks]` The decrypting node can also obtain $C_3^{**}$ from the second part ($b-d$ bits) of $D_K(C_4) \oplus (C_3^* \,||\, \mathbf{0})$. Therefore, it obtains $C_3^* \,||\, C_3^{**}$. Describe how it obtains $P_3$ from $C_3^* \,||\, C_3^{**}$.

5. [8 marks] (Extension attack against hash functions) Consider two messages to be hashed by a cryptographic hash function $h()$. The size of the first message $m_1$ is *not* a multiple of the hash function's block size. The size of the second message $m_2$, on the other hand, is a multiple of the hash function's block size. The hash function uses this padding method: *Always* pad with a bit 1 and then followed by a minimal number of bit 0 (the one considered in assignment 1).

   Would the following padding attacks be successful, assuming that an attacker has already obtained $m_1$ and $h(m_1)$, and $m_2$ and $h(m_2)$? Support your answers with concrete explanation.

   (a) [2 marks] An attacker crafts a new message $m_1 \mid\mid m_3$, such that $m_3$ is arbitrarily selected to fill $m_1$ with just enough data for meeting the block size requirement.

   (b) [2 marks] Same as (a) (i.e., $m_1 \mid\mid m_3$). Additionally, he concatenates it with $m_4$ (i.e., $m_1 \mid\mid m_3 \mid\mid m_4$) which generally *does not* comprise a multiple of blocks.

   (c) [2 marks] An attacker crafts a new message $m_2 \mid\mid m_3$, where $m_3$ is arbitrarily selected, and it comprises a multiple of blocks.

   (d) [2 marks] An attacker crafts a new message $m_2 \mid\mid m_3$, where $m_3$ is arbitrarily selected, and it *does not* comprise a multiple of blocks.

6. [10 marks] (A hash-based password system) Consider the following password scheme for Bob to authenticate Alice. First we denote $hash^n(\texttt{passwd}) = hash(hash^{n-1}(\texttt{passwd})), n > 1$ and $hash^1(\texttt{passwd}) = hash(\texttt{passwd})$.

   When Alice registers her password for the first time, she picks a large $n$ randomly, and computes $hash^n(\texttt{passwd})$. She then sends her identity, the hash value and $n$ to Bob. Assume that Bob and Alice have agreed on a secure one-way hash function beforehand. Moreover, Alice does not remember $n$ and the hash value.

   When she logins again next time,

   (a) Alice (or someone else) $\rightarrow$ Bob: "I am Alice."

   (b) Bob $\rightarrow$ Alice: $n$.

   (c) Alice $\rightarrow$ Bob: $hash^{n-1}(\texttt{passwd})$.

   (d) Bob hashes $hash^{n-1}(\texttt{passwd})$ once and compares it with the stored $hash^n(\texttt{passwd})$ for Alice.

      i. If they match, the authentication succeeds. Bob then replaces the stored $hash^n(\texttt{passwd})$ and $n$ with $hash^{n-1}(\texttt{passwd})$ and $n-1$, respectively.

      ii. Otherwise, the authentication fails.

   Thus, $n$ decreases each time Alice logins successfully.

   (a) [6 marks] Consider that Eve can read the three login (unencrypted) messages between Alice and Bob. How does the preimage-resistant property of the one-way hash function prevent Eve from logging-in successfully as Alice?

   (b) [4 marks] Not only Eve can observe the login messages, she can also launch an active attack. For example, Eve can capture the 2nd message and changes $n$ to a smaller

value, say $n'$, and forwards the modified message to Alice. Moreover, Eve receives $hash^{n'-1}(\texttt{passwd})$ from Alice. Discuss how Eve can impersonate Alice with that information.

7. `[6 marks]` (The Chinese Remainder Theorem, CRT) We re-visit an assignment problem on the CRT. Consider $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, and $P = p_1 \times p_2 \times p_3 = 30$, and $x \in \{0, 1, 2, \cdots, 29\}$. We would like to compute $12^{9999}$ *mod* 30. We know that by the CRT, $12^{9999}$ *mod* 30 can be represented by $(0 \ mod \ 2, 0 \ mod \ 3, 12^{9999} \ mod \ 5)$.

   (a) `[4 marks]` What is the value of $12^{9999}$ *mod* 5? (Hint: $12^4 \equiv 1 \ (mod \ 5)$).

   (b) `[2 marks]` What is the value of $12^{9999}$ *mod* 30? (Hint: solving the CRT by setting $P_3 = 6$ and $y_3 = 1$ in the formula on slide 25 of Prelude to Public-Key Cryptography).

8. `[6 marks]` (Affine cipher) Consider Affine cipher with $Z_{233}$. What is the key size of the key space for this cipher (Hint: an example in slide 10 of Prelude to Public-Key Cryptography, and 233 is a prime.).