Software Security 2024-2025 Fall
Assignment 2: Encryption Operation Modes

Deadline: 9/12/2024

הוראות הגשה: (אי קיום הוראות אלו עלול לגרום להורדת ציון!)

1. **תאריך הגשה: 9.12.2024 בשעה 23:55 למטלה הקשורה ב-Moodle בלבד.**
2. **יש להגיש קובץ PDF אחד, מרוכז, ברור ונקי. (ציון יורד אם אין סדר וניקיון ואי הגשה בקובץ PDF!)**
3. **אין להגיש בשום פנים ואופן למייל של מרצה או מתרגל - אך ורק ב-Moodle.**
4. **דחיית העבודה ניתנת רק במקרה של מילואים או אישור מחלה. יש להגיש בקשת סטודנט בצירוף המסמכים. אין לפנות במייל למתרגל או למרצה בבקשת דחיית העבודה!**
5. **ניתן להגיש את העבודה בזוגות בלבד.**
6. **לא יתקבלו עבודות שהוגשו באיחור.**
7. **ניתן לערער תוך 3 ימים בלבד לאחר פרסום ציונים!**
8. **במקרה של העתקה מלאה או חלקית של העבודה (מסטודנטים אחרים, מ-Internet או מכל מקום אחר), יינתן ציון 0 על העבודה של כלל הסטודנטים המעורבים והם יעלו לוועדת משמעת. במקרה שהתגלתה העתקה, אנו שומרים את הזכות לבדוק העתקות גם בעבודות קודמות.**

Preliminaries

The following questions review Triple DES (3DES) and Operation Modes. Triple DES (3DES), is a symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm.

Triple DES uses a "key bundle" that comprises three DES keys, K1, K2 and K3, each of 56 bits (excluding parity bits). The encryption algorithm is:

```
ciphertext = EK3(DK2(EK1(plaintext)))
```

i.e., DES encrypt with K1, DES decrypt with K2, then DES encrypt with K3.

Three keying options are standardized:

1. Keying option 1: $K_1 \neq K_2 \neq K_3$
2. Keying option 2: $K_1 = K_3$
3. Keying option 3: $K_1 = K_2 = K_3$

1. Why is the middle portion of 3DES a decryption rather than an encryption?

2. Fill in the remainder of this table and explain briefly:

Mode	Encrypt	Decrypt
ECB	$C_j = E(K, P_j), j = 1, \dots, N$	$P_j = D(K, C_j), j = 1, \dots, N$
CBC	$C_1 = E(K, [P_1 \oplus IV])$ $C_j = E(K, [P_j \oplus C_{j-1}]), j = 2, \dots, N$	$P_1 = D(K, C_1) \oplus IV$ $P_j = D(K, C_j) \oplus C_{j-1}, j = 2, \dots, N$
CFB		
OFB		
CTR		

3. You want to build a hardware device to do block encryption in the cipher block chaining (CBC) mode using an algorithm stronger than DES. 3DES is a good candidate. Figure 1 below shows two possibilities, both of which follow from the definition of CBC. Which of the two would you choose:

a. For security ?

b. For performance ?

Explain.

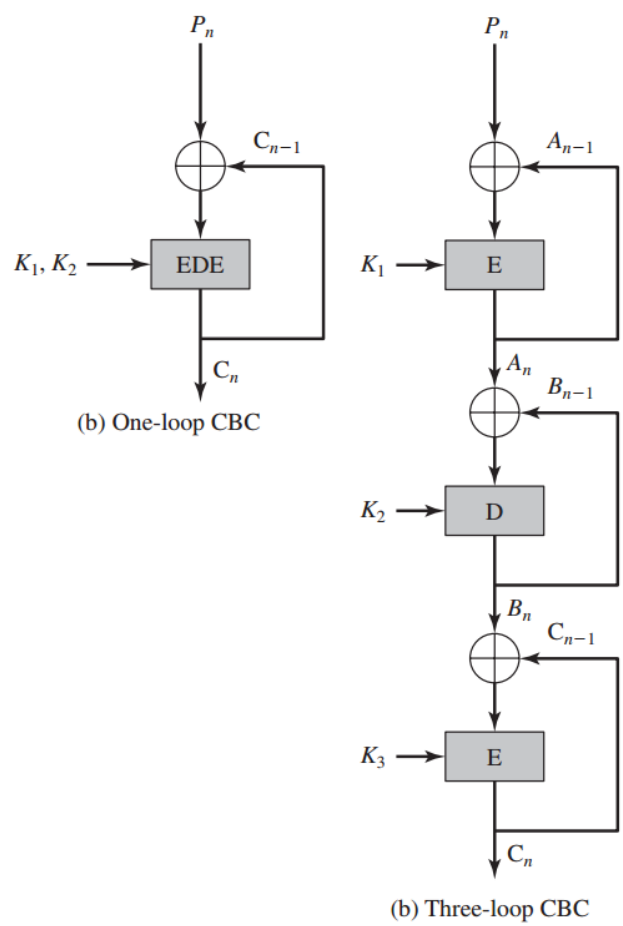

Figure 1

4. Consider the following encryption mode for applying AES-128 with a key K to a message M that consists of l 128-bit blocks, $M_1, \dots, M_l$. The sender first picks a random 128-bit string C_0, which is the first block of ciphertext. Then for $i > 0$, the ith ciphertext block is given by $\mathrm{C}_i = C_{i-1} \oplus \text{AES-128}_K(M_i)$. The ciphertext is the concatenation of these individual blocks: $\mathrm{C} = \mathrm{C}_0 || C_1 || \dots || C_l$.

a. Explain what is the intent behind the random value C_0 ?
b. Is this mode of encryption secure ? Briefly explain your answer.
c. Suppose we replace the computation of C_i with $\mathrm{C}_i = \text{AES-128}_K(C_{i-1} \oplus M_i)$. Does this make the mode of encryption more secure, less secure, or unchanged ? Briefly explain your answer.

5. With the ECB mode of DES, if there is an error in a block of the transmitted ciphertext, only the corresponding plaintext block is affected. However, in the CBC mode, this error propagates. For example, an error in the transmitted C_1 (see Figure 2) obviously corrupts decryption of P_1 and P_2.

a. Are any blocks beyond P_2 are affected ?
b. Suppose that there is a bit error in the source version of P_1. Through how many ciphertext blocks is this error propagated? What is the effect at the receiver ?

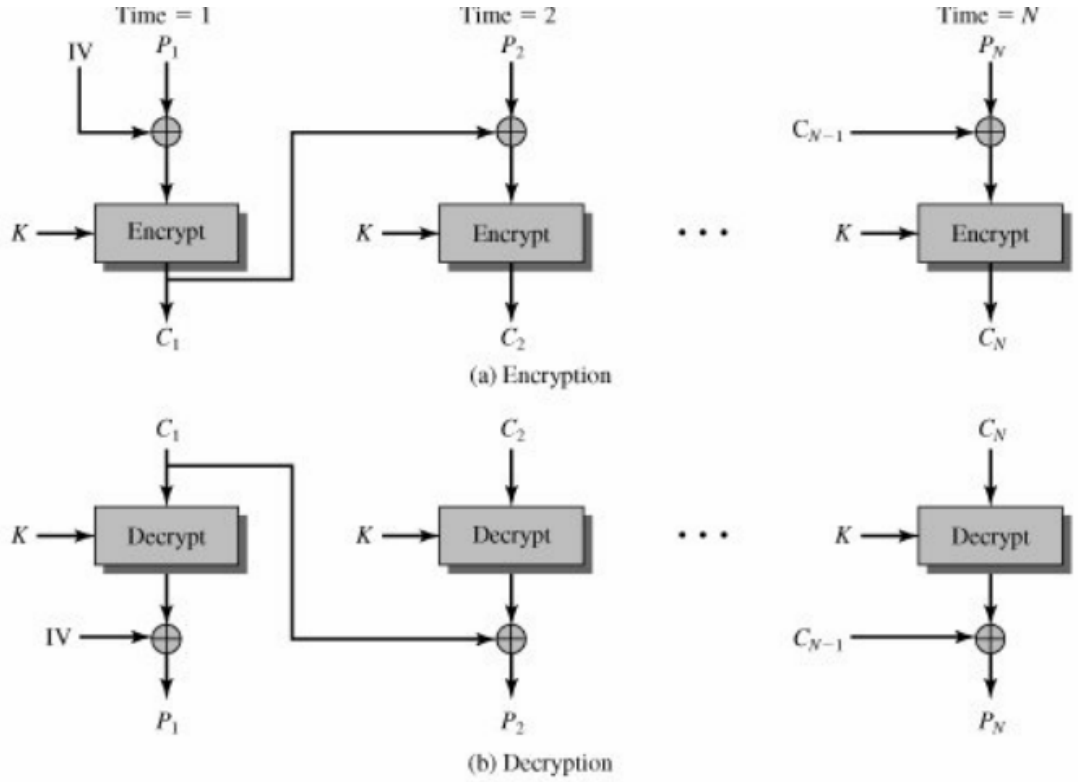
Time = 1
Time = 2
Time = N
IV
P_1
P_2
P_N
C_{N-1}
K
Encrypt
C_1
C_2
C_N
(a) Encryption
Decrypt
(b) Decryption

Figure 2