TCSS 581 Cryptology

Homework 4

Tianyi Li
Student ID: 1827924

Tianyi Li
Student #:1827924

1 Encrypt the King James Bible using:

a. **AES in CBC mode of operation**
b. **AES in Counter Mode of Operation**
c. **DES in CBC Mode of Operation**
d. **DES in Counter Mode of Operation**
e. **3DES in CBC Mode of Operation**
f. **3DES in Counter Mode of Operation**

Provide your code and the times for encryption and decryption. For which of these modes of operation can you improve the running times by exploiting parallelization?

- For the code and running times, check out the other file, *code.pdf*.
- Both of the modes, CBC and Counter (CTR), support parallel decryption, but only CTR can parallelize encryption.
- Decryption using CBC requires access to the previous block of ciphertext, which is defined as this

$$m_i := F_k{}^{-1}(c_i) \oplus c_{i-1}$$

- There will be an issue if it cannot access to the previous block, such that it cannot start decrypt the next block until the previous one has done processing.
- One the other hand, the parallelizability of the CTR mode can often makes it go faster, comparing to other modes.

2 Show that a CBC mode of operation is not CPA secure if the initialization vector is not random and kept constant.

- The encryption using the CBC mode is defined as

$$c_i = F_k(c_{i-1} \oplus m_i)$$

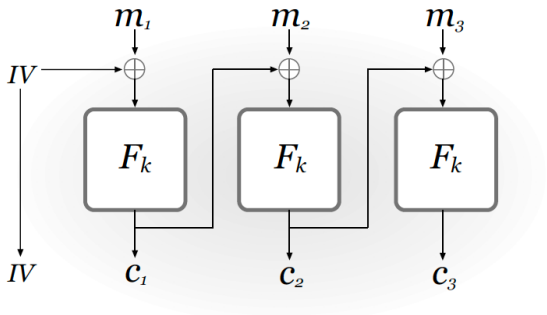

FIGURE 3.7: Cipher Block Chaining (CBC) mode.

- An initialization vector (IV) in this case works as the initial c_i, that is c_0, such that

$$c_1 = F_k(c_0 \oplus m_1)$$

- Which is the same as

$$c_1 = F_k(IV \oplus m_1)$$

- When looking at the CBC diagram, having a fixed IV is equivalent to having the first ciphertext block become the IV.
- If the adversary A can choose what plaintext they wanted to see (CPA), and the IV in this case is unknow, but has been kept constant, A can draw up a possible attack on guessing prefixes of the unknown plaintext and encrypting it, to see if they match.
- A would be possible to observe if $IV \oplus m_1$ would result in identical input to the block cipher, resulting in identical ciphertext.
- Therefore, using a predictable IV could leak information about previous plaintext having a specific value.
- To illustrate:
  - Let there be two plaintext messages $m_1 = '0000'$ and $m_2 = '0001'$, and two IVs that in increment with the two messages, such that $IV_1 = '0000'$ and $IV_2 = '0001'$.
  - Let the message $m_1 = '0000'$ uses the IV $IV_1 = '0000'$,
  - Then the input to the block cipher is $'0000'$.
  - Suppose we encrypt the message $m_2 = '0001'$ uses the IV $IV_2 = '0001'$,
  - Since $0001 \oplus 0001 = 0000$,
  - Then, this input to the block cipher to be the same as before, $'0000'$.
  - Then, both messages would produce to the same ciphertext.
  - Since A can use a CPA attack on this scheme, A knows that $m_1$and m_2 are different,
  - Then A can learn that they were different (since the IV is different, but the ciphertexts are the same).
  - Therefore, non-random IVs are more likely to correlate with the plaintext and leak information.
- Thus, the CBC mode of operation is not CPA secure if the initialization vector is not random and kept constant.

3 Let F be a pseudorandom function and G be a pseudorandom generator with expansion factor $\ell(n) = n + 1$. For each of the following encryption schemes, state whether the scheme has indistinguishable encryptions in the presence of an eavesdropper and whether it is CPA-secure. (In each case, the shared key is a uniform $k \in \{0,1\}^n$.) Explain your answer.

(a) To encrypt $m \in \{0,1\}^{2n+2}$, parse m as $m_1 \parallel m_2$ with $|m_1| = |m_2|$ and send $\langle G(k) \oplus m_1, G(k+1) \oplus m_2 \rangle$.

- This scheme is CPA-secure, such that it is similar to the correctness proof of CTR mode (Theorem 3.32 from textbook) with only two blocks.
- Thus, it has indistinguishable encryptions in the presence of an eavesdropper as well.

(b) To encrypt $m \in \{0,1\}^{n+1}$, choose uniform $r \leftarrow \{0,1\}^n$ and output the ciphertext $\langle r, G(r) \oplus m \rangle$.

- This scheme has indistinguishable encryptions in the presence of an eavesdropper.
- Since an adversary A is given the ciphertext, also the encryption function also does not use a key.
- By first compute $G(r)$, then $G(r) \oplus (G(r) \oplus m) = m$.
- Therefore, an adversary can easily the decrypt the ciphertext in polynomial time without knowing the key, just as the legit receiver.
- The scheme is also not CPA-secure, since the encryption is deterministic and the reasons above.

(c) To encrypt $m \in \{0,1\}^n$, output the ciphertext $m \oplus F_k(0^n)$.

- This scheme has indistinguishable encryptions.
- Therefore, it is secure in the presence of an eavesdropper.
- The scheme is not CPA-secure, since the encryption is deterministic.
- Then it does not even have indistinguishable encryptions for multiple messages.

(d) To encrypt $m \in \{0,1\}^{2n}$, parse m as $m_1 \parallel m_2$ with $|m_1| = |m_2|$, then choose $r \leftarrow \{0,1\}^n$ at random, and send $\langle r, m_1 \oplus F_k(r), m_2 \oplus F_k(r+1) \rangle$.

- This scheme is CPA-secure, such that it is similar to the correctness proof of CTR mode (Theorem 3.32 from textbook) with only two blocks.
- Thus, it has indistinguishable encryptions in the presence of an eavesdropper as well.

4 Present formulas for decryption of all the different modes of encryption we have seen. For which modes can decryption be parallelized?

- These are the different modes we have learnt (textbook has covered) and their formulas:

Mode	*Decryption Formula*	*Parallelizable?*
ECB	$m_i := F_k{}^{-1}(c_i)$	Yes
CBC	$c_0 := IV$ $m_i := F_k{}^{-1}(c_i) \oplus c_{i-1}$	Yes, but not that efficient
OFB	$y_0 := IV$ $y_i := F_k(y_{i-1})$ $m_i := y_i \oplus c_i$	No
CTR	counter ctr $y_i := F_k(ctr + i)$, where ctr and i are viewed as integers and addition is done modulo 2^n $m_i := y_i \oplus c_i$	Yes

Challenge **Let $\Pi_1 = (Gen_1, Enc_1, Dec_1)$ and $\Pi_2 = (Gen_2, Enc_2, Dec_2)$ be two encryption schemes for which it is known that at least one is CPA-secure. The problem is that you don't know which one is CPA-secure and which one may not be. Show how to construct an encryption scheme Π that is guaranteed to be CPA-secure as long as at least one of Π_1 or Π_2 is CPA-secure. Try to provide a full proof of your answer.**

- Let $M = \{0,1\}^n$ be the message space.
- And there is an encryption scheme $\Pi = (Gen, Enc, Dec)$, such that
  - Gen : inputs 1^n , run Gen_1 and Gen_2 , and outputs a key $k = (k_1, k_2)$, where Gen_1 generates k_1 and Gen_2 generates k_2.
  - Enc: inputs the keys $k = (k_1, k_2)$, a message $m \in \{0,1\}^n$, and r such that $r \leftarrow \{0,1\}^n$ uniformly at random, and output the ciphertext $c = (c_1, c_2)$ as
    $$c := (Enc_{1,k_1}(r), Enc_{2,k_2}(m \oplus r))$$
  - Dec: inputs the keys $k = (k_1, k_2)$ and a ciphertext $c = (c_1, c_2)$, and outputs the plaintext message $m := Dec_{1,k_1}(c_1) \oplus Dec_{2,k_2}(c_2)$.

- **Proof**: the proposed encryption scheme $\Pi = (Gen, Enc, Dec)$ is CPA secure.
  - Let Π_1 to be the one that is CPA-secure and Π_2 is not,
  - Suppose there is an adversary A, who might be able to recover $m \oplus r$, but not just r.
  - Then so far, A still cannot find any information regarding the message m.
  - Because r was chosen at random and r is still secure, given that Π_1 is CPA-secure, $m \oplus r$ looks completely random to A,
  - This is now similar to the one-time pad.
  - Since it is impossible to distinguish between two messages m_0 and m_1, where $m_0 \neq m_1$, under Π
  - Then A cannot learn anything about the pad that r used.
  - Therefore, Π is CPA-secure.

  - Vice versa, let Π_2 to be the one that is CPA-secure and Π_1 is not,
  - And A might be able to find out what r is, but cannot figure out what $m \oplus r$ is.
  - Then A still cannot find any information regarding the message m.
  - Because it is impossible to distinguish between two messages m_0 and m_1 , where $m_0 \neq m_1$, under Π,
  - Therefore A cannot distinguish between $m_0 \oplus r$ and $m_1 \oplus r$, since r might be known already.
  - Since it is given that Π_2 is CPA-secure,
  - Hence, Π is CPA-secure.
- Thus, Π is guaranteed to be CPA-secure, as long as at least one of Π_1 or Π_2 is CPA-secure.