Madison & Ana
Summer 2023

CS 161 Computer Security

Exam Prep 4

Q1 *AES-161* (23 points)

Alice has created a scheme called AES-161 to send messages to Bob securely in the presence of a man-in-the-middle attacker Mallory. Alice and Bob both share a symmetric key K that is secret from everyone else.

The encryption scheme for AES-161 is as follows:

$$\begin{aligned} C_1 &= E_K(IV_1 \oplus M_1) \\ C_2 &= E_K(C_1 \oplus IV_2 \oplus M_2) \\ C_i &= E_K(C_{i-1} \oplus C_{i-2} \oplus M_i) \end{aligned}$$

Q1.1 (3 points) Write the decryption formula of AES-161 for M_i, for $i > 2$.

Solution: $M_i = D_K(C_i) \oplus C_{i-1} \oplus C_{i-2}$

Solve this by beginning with the encryption formula for M_i and isolating M_i to its own side.

$$\begin{aligned} C_i &= E_K(C_{i-1} \oplus C_{i-2} \oplus M_i) & \\ D_K(C_i) &= C_{i-1} \oplus C_{i-2} \oplus M_i & \text{(Call } D_K \text{ on both sides)} \\ D_K(C_i) \oplus C_{i-1} &= C_{i-2} \oplus M_i & \text{(XOR } C_{i-1} \text{ on both sides)} \\ D_K(C_i) \oplus C_{i-1} \oplus C_{i-2} &= M_i & \text{(XOR } C_{i-2} \text{ on both sides)} \end{aligned}$$

Verify this solution:

$$\begin{aligned} & D_K(C_i) \oplus C_{i-1} \oplus C_{i-2} \\ &= D_K(E_K(C_{i-1} \oplus C_{i-2} \oplus M_i)) \oplus C_{i-1} \oplus C_{i-2} \\ &= C_{i-1} \oplus C_{i-2} \oplus M_i \oplus C_{i-1} \oplus C_{i-2} \\ &= C_{i-1} \oplus C_{i-2} \oplus M_i \oplus C_{i-1} \oplus C_{i-2} \\ &= M_i \end{aligned}$$

Q1.2 (4 points) Is this scheme IND-CPA secure with randomly generated IVs? If you mark “Yes”, provide a brief justification (10 words or fewer; no formal proof necessary). If you mark “No”, provide a strategy to win the IND-CPA game with probability greater than $1/2$.

● Yes ○ No

Solution: The scheme is IND-CPA secure with randomly generated IVs. Since E_K is a block cipher, its output is a pseudorandom permutation as long as the inputs are unique. Since the IVs are guaranteed to be random, even using the same messages will result in the input to the block cipher being unique, therefore implying that the output will be a pseudorandom permutation, making it indistinguishable from random.

Consider the following attack, called the FEI attack:

Given a ciphertext C of a known plaintext M, Mallory wishes to provide C' such that some subset of blocks of Mallory's choosing would be decrypted to M'_i, where both i and M'_i are **any values of Mallory's choosing**. For other values of i, the corresponding M'_is **can be anything**.

For example, let's say Mallory wants to provide a C' so that the first and last blocks of an 8-block message are decrypted into values M'_1 and M'_8 of her choosing while blocks 2 through 7 are not necessarily values of her choosing. In other words, when Bob decrypts the ciphertext C', he will get

$$M'_1 \| x_1 \| x_2 \| x_3 \| x_4 \| x_5 \| x_6 \| M'_8$$

where x_i refers to any value.

Q1.3 (6 points) Alice wishes to send a 3-block message M. Mallory wants to perform the FEI attack on the third block.

Provide a formula for all C'_i that differ from their corresponding C_i in terms of M_i, C_i, M'_i, and C'_i for specific values of i. Your formula may also include any public values. You don't need to provide a formula for any $C'_i = C_i$.

Solution: Any answer that sets $C'_3 = C_3$ and chooses C'_1 and C'_2 such that

$$C'_1 \oplus C'_2 = C_1 \oplus C_2 \oplus M_3 \oplus M'_3$$

is valid. We show this by running Bob's decryption process on the third block.

To get the plaintext for the third-block given C'_i, Bob will compute $D_K(C'_3) \oplus C'_2 \oplus C'_1$ (using the decryption formula from part one). Using our assumption that $C'_3 = C_3$ and $C'_1 \oplus C'_2 = C_1 \oplus C_2 \oplus M_3 \oplus M'_3$, we get that

$$\begin{aligned}
\text{Third Block's Plaintext} &= D_K(C'_3) \oplus C'_2 \oplus C'_1 \\
&= D_K(C_3) \oplus C_1 \oplus C_2 \oplus M_3 \oplus M'_3 \\
&= D_K(E_K(M_3 \oplus C_2 \oplus C_1)) \oplus C_1 \oplus C_2 \oplus M_3 \oplus M'_3 \\
&= M_3 \oplus C_2 \oplus C_1 \oplus C_1 \oplus C_2 \oplus M_3 \oplus M'_3 \\
&= M_3 \oplus C_2 \oplus C_1 \oplus C_1 \oplus C_2 \oplus M_3 \oplus M'_3 \\
&= M'_3
\end{aligned}$$

Thus, Bob will decrypt the third block as plaintext as M'_3 as desired.

Common Correct Answers:

- $C'_1 = C_1 \oplus M_3 \oplus M'_3$, $C'_2 = C_2$, $C'_3 = C_3$
- $C'_1 = C_1$, $C'_2 = C_2 \oplus M_3 \oplus M'_3$, $C'_3 = C_3$
- $C'_1 = C_1 \oplus C_2 \oplus M_3 \oplus M'_3$, $C'_2 = 0$, $C'_3 = C_3$
- $C'_1 = 0$, $C'_2 = C_1 \oplus C_2 \oplus M_3 \oplus M'_3$, $C'_3 = C_3$

Q1.4 (5 points) Assume that Alice is sending a 9-block message. What is the maximum number of blocks that Mallory can perform the FEI attack on?

Solution: 4. It is blocks 1, 3, 5, and 7. Or block 2, 4, 6, and 8.

Q1.5 (5 points) Assume that Alice is sending a 9-block message. Mallory wants to perform the FEI attack on the maximum number of blocks. You can pick which blocks the FEI attack is performed on.

Provide a formula for all C'_i that differ from their corresponding C_i in terms of M_i, C_i, M'_i, and C'_i for specific values of i. Your formula may also include any public values. You don't need to provide a formula for any $C'_i = C_i$.

Solution: Our original intention for this question was to modify the IV to be $IV' = IV \oplus M_1 \oplus M'_1$ first. Then, the attack would be $C'_i = C_i \oplus M_{i+1} \oplus M'_{i+1}$ for i in [2, 4, 6, 8], thus making a total of 5 modified blocks.

However, we felt as though we did not make it clear enough that the IV could be modified, and therefore the actual solution for this problem would be to modify $C'_i = C_i \oplus M_{i+1} \oplus M'_{i+1}$ for one of the following:

- i in [2, 4, 6, 8]
- i in [1, 3, 5, 7]

Q2 *AES-GROOT* (30 points)

Tony Stark develops a new block cipher mode of operation as follows:

$$\begin{aligned} C_0 &= IV \\ C_1 &= E_K(K) \oplus C_0 \oplus M_1 \\ C_i &= E_K(C_{i-1}) \oplus M_i \\ C &= C_0 \| C_1 \| \cdots \| C_n \end{aligned}$$

For all parts, assume that IV is randomly generated per encryption unless otherwise stated.

Q2.1 (3 points) Write the decryption formula for M_i using AES-GROOT. You don't need to write the formula for M_1.

Solution:

$$\begin{aligned} M_1 &= C_1 \oplus E_K(K) \oplus IV \\ M_i &= C_i \oplus E_K(C_{i-1}) \end{aligned}$$

Q2.2 (3 points) AES-GROOT is not IND-CPA secure. Which of the following most accurately describes a way to break IND-CPA for this scheme?

● It is possible to compute a deterministic value from each ciphertext that is the same if the first blocks of the corresponding plaintexts are the same.

○ C_1 is deterministic. Two ciphertexts will have the same C_1 if the first blocks of the corresponding plaintexts are the same.

○ It is possible to learn the value of K, which can be used to decrypt the ciphertext.

○ It is possible to tamper with the value of IV such that the decrypted plaintext block M_1 is mutated in a predictable manner.

Solution: The first block of ciphertext is, in fact, non-deterministic since it's XORed with a random IV. However, this doesn't provide any useful security since it's easy to just XOR out the IV and reveal the value of $E_K(K) \oplus M_1$, which is deterministic.

It is not possible to leak the value of K, and tampering with the IV does break integrity, but this does not inherently violate IND-CPA (though it might break other threat models such as IND-CCA).

Q2.3 (5 points) AES-GROOT is vulnerable to plaintext recovery of the first block of plaintext. Given a ciphertext C of an unknown plaintext M and different plaintext-ciphertext pair (M', C'), provide a formula to recover M_1 in terms of C_i, M'_i, and C'_i (for any i, e.g. C_0, M'_2, C'_6).

Recall that the IV for some ciphertext C can be referred to as C_0.

Solution: Like previously, we can XOR out the value of $C_0 = IV$, and, because we know the value of C'_1 and M'_1 in our plaintext-ciphertext pair, we can derive the value of $E_K(K) = C'_1 \oplus C'_0 \oplus M'_1$. Thus, to learn M_1, we compute

$$\begin{aligned} M_1 &= C_1 \oplus C_0 \oplus C'_1 \oplus C'_0 \oplus M'_1 \\ &= (E_K(K) \oplus C_0 \oplus M_1) \oplus C_0 \oplus (E_K(K) \oplus C'_0 \oplus M'_1) \oplus C'_0 \oplus M'_1 \\ &= M_1 \end{aligned}$$

If AES-GROOT is implemented with a fixed $IV = 0^b$ (a fixed block of b 0's), the scheme is vulnerable to full plaintext recovery under the chosen-plaintext attack (CPA) model. Given a ciphertext C of an unknown plaintext and different plaintext-ciphertext pair (M', C'), describe a method to recover plaintext block M_4.

Q2.4 (5 points) First, the adversary sends a value M'' to the challenger. Express your answer in terms of in terms of C_i, M'_i, and C'_i (for any i).

Solution: We need to learn the value of $E_K(C_3)$ in order to recover the value of M_4. Since the IV is fixed at 0^b, we can send some message with $M''_1 = E_K(K) \oplus C_3$ and $M''_2 = 0^b$ ino rder to learn the $E_K(C_3)$. To do this, we first need to derive an expression for $E_K(K)$. Given (M', C'), we know that we can XOR out M'_1 from C'_1 to arrive at

$$\begin{aligned} E_K(K) &= C'_1 \oplus M'_1 \\ &= E_K(K) \oplus 0^b \oplus M'_1 \oplus M'_1 \\ &= E_K(K) \end{aligned}$$

Once we have this expression, we send

$$\begin{aligned} M''_1 &= C'_1 \oplus M'_1 \oplus C_3 \\ M''_2 &= 0^b \\ M'' &= M''_1 \| M''_2 \end{aligned}$$

The first block of the resulting ciphertext is $C''_1 = E_K(K) \oplus 0^b \oplus E_K(K) \oplus C_3 = C_3$. Because of this, the second resulting ciphertext block is $C''_2 = E_K(C_3) \oplus 0^b = E_K(C_3)$.

Q2.5 (5 points) The challenger sends back the encryption of M'' as C''. Write an expression for M_4 in terms of C_i, M_i', C_i', M_i'', and C_i'' (for any i).

Solution: Now that we have $C_2'' = E_K(C_3)$, we can simply XOR out that value from $C_4 = E_K(C_3) \oplus M_4$. The resulting expression is

$$\begin{aligned} M_4 &= C_4 \oplus C_2'' \\ &= E_K(C_3) \oplus M_4 \oplus E_K(C_3) \\ &= M_4 \end{aligned}$$

Q2.6 (4 points) Which of the following methods of choosing IV allows an adversary under CPA to fully recover an arbitrary plaintext (not necessarily using your attack from above)? Select all that apply.

□ IV is randomly generated per encryption

■ $IV = 1^b$ (the bit 1 repeated b times)

■ IV is a counter starting at 0 and incremented per encryption

■ IV is a counter starting at a randomly value chosen once during key generation and incremented per encryption

□ None of the above

Solution: The above attack is possible with any method of choosing IV that's predictable.

Q2.7 (2 points) Let C be the encryption of some plaintext M. If Mallory flips with the last bit of C_3, which of the following blocks of plaintext no longer decrypt to its original value? Select all that apply.

□ M_1

□ M_2

■ M_3

■ M_4

□ None of the above

Solution: We see M_i depends on C_i and C_{i-1}. That implies that a change in C_3 will result in a change of M_3 and M_4.

Q2.8 (3 points) Which of the following statements are true for AES-GROOT? Select all that apply.

- □ Encryption can be parallelized
- ■ Decryption can be parallelized
- □ AES-GROOT requires padding
- □ None of the above

Solution: Decryption can be parallelized because ciphertext decryption does not depend on another plaintext block. However, encryption depends on a previous ciphertext block, so it cannot be parallelized.

Padding is not required because the plaintext blocks are simply XORed with the encryption of the previous ciphertext block, like in CFB.