## CS 161 Computer Security

Exam Prep 4

(30 points)

## Q1 AES-GROOT

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

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

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

Q1.1 (3 points) Write the decryption formula for  $M_i$  using AES-GROOT. You don't need to write the formula for  $M_1$ .

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

- Q1.2 (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.
  - $\bigcirc$   $C_1$  is deterministic. Two ciphertexts will have the same  $C_1$  if the first blocks of the corresponding plaintexts are the same.
  - $\bigcirc$  It is possible to learn the value of K, which can be used to decrypt the ciphertext.
  - $\bigcirc$  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).

Q1.3 (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

 $M_1 = C_1 \oplus C_0 \oplus C'_1 \oplus C'_0 \oplus M'_1$ =  $(E_K(K) \oplus C_0 \oplus M_1) \oplus C_0 \oplus (E_K(K) \oplus C'_0 \oplus M'_1) \oplus C'_0 \oplus M'_1$ =  $M_1$  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  $M_4$ .

Q1.4 (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

$$E_K(K) = C'_1 \oplus M'_1$$
  
=  $E_K(K) \oplus 0^b \oplus M'_1 \oplus M'_1$   
=  $E_K(K)$ 

Once we have this expression, we send

$$M_{1}'' = C_{1}' \oplus M_{1}' \oplus C_{3}$$
$$M_{2}'' = 0^{b}$$
$$M'' = M_{1}'' \|M_{2}''$$

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  $C_2'' = E_K(C_3) \oplus 0^b = E_K(C_3)$ .

Q1.5 (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*).

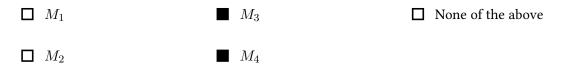
**Solution:** Now that we have  $C_2'' = E_K(C_3)$ , we can simply XOR out that value from  $C_4 = E_K(C_3) \oplus M_4$ . The resulting expression is

$$M_4 = C_4 \oplus C_2''$$
  
=  $E_K(C_3) \oplus M_4 \oplus E_K(C_3)$   
=  $M_4$ 

- Q1.6 (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.
  - $\Box$  *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
  - $\blacksquare$  *IV* is a counter starting at a randomly value chosen once during key generation and incremented per encryption
  - $\Box$  None of the above

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

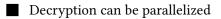
Q1.7 (2 points) Let C be the encryption of some plaintext M. If Mallory flips with the last bit of  $C_3$ , which of the following blocks of plaintext no longer decrypt to its original value? Select all that apply.



**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  $M_4$ .

Q1.8 (3 points) Which of the following statements are true for AES-GROOT? Select all that apply.

**Encryption** can be parallelized



- □ AES-GROOT requires padding
- $\hfill\square$  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.