Midterm review

CS 161
Raluca Ada Popa
Feb 19, 2020
Fall 18, Midterm 1

Problem 9  **Screwups in Inserting an IV**  (15 points)

Alice encrypts two messages, $M_1$ and $M_2$ using the same IV/nonce and a deterministic padding scheme (when appropriate for the particular mode) using AES (a 128b block cipher). Eve, the Eavesdropper, knows the plaintext of $M_1$, that each block of $M_1$ is different, that $M_1$ is 120 bytes, and that Alice never sends any bytes she doesn’t have to. Unbeknownst to Eve, it turns out that the messages differ only in the 21st byte of the two messages but are otherwise identical.

Yes, Alice screwed up. But how badly? For each possibility, select *all* which apply.

(a) If Alice used AES-ECB (Electronic Code Book), Eve is able to determine which of the following about $M_2$:

- [ ] That $M_2$ is exactly 120B long
- [ ] That $M_2$ is less than 129B long but not the exact length
- [ ] The entire plaintext for $M_2$
- [ ] The plaintext for only the first two blocks of $M_2$
- [ ] The entire plaintext for $M_2$ except for the 2nd block
- [ ] The plaintext for only the first block of $M_2$
Problem 9  *Screwups in Inserting an IV*  

Alice encrypts two messages, $M_1$ and $M_2$ using the same IV/nonce and a deterministic padding scheme (when appropriate for the particular mode) using AES (a 128b block cipher). Eve, the Eavesdropper, knows the plaintext of $M_1$, that each block of $M_1$ is different, that $M_1$ is 120 bytes, and that Alice never sends any bytes she doesn’t have to. Unbeknownst to Eve, it turns out that the messages differ only in the 21st byte of the two messages but are otherwise identical.

Yes, Alice screwed up. But how badly? For each possibility, select *all* which apply.

**Q:** How many blocks is M1?  
**A:** Each block is $128/8=16$ bytes long, so M1 is more than 7 blocks: 8 blocks with padding

**Q:** Which block contains the 21st byte?  
**A:** The second block. So the messages differ only in the in second block.
Recall ECB Encryption

break message M into $P_1|P_2|...|P_m$ each of n bits (block cipher input size)

\[
\text{Enc}(K, P_1|P_2|...|P_m) = (C_1, C_2, ..., C_m)
\]
Problem 9  *Screwups in Inserting an IV*  

Alice encrypts two messages, $M_1$ and $M_2$ using the same IV/nonce and a deterministic padding scheme (when appropriate for the particular mode) using AES (a 128b block cipher). Eve, the Eavesdropper, knows the plaintext of $M_1$, that each block of $M_1$ is different, that $M_1$ is 120 bytes, and that Alice never sends any bytes she doesn’t have to. Unbeknownst to Eve, it turns out that the messages differ only in the 21st byte of the two messages but are otherwise identical.

Yes, Alice screwed up. But how badly? For each possibility, select *all* which apply.

(a) If Alice used AES-ECB (Electronic Code Book), Eve is able to determine which of the following about $M_2$:

- That $M_2$ is exactly 120B long
- The entire plaintext for $M_2$
- The entire plaintext for $M_2$ except for the 2nd block
- That $M_2$ is less than 129B long but not the exact length
- The plaintext for only the first two blocks of $M_2$
- The plaintext for only the first block of $M_2$
Fall 18, Midterm 1

Problem 9  Screwups in Inserting an IV  

Alice encrypts two messages, $M_1$ and $M_2$ using the same IV/nonce and a deterministic padding scheme (when appropriate for the particular mode) using AES (a 128b block cipher). Eve, the Eavesdropper, knows the plaintext of $M_1$, that each block of $M_1$ is different, that $M_1$ is 120 bytes, and that Alice never sends any bytes she doesn’t have to. Unbeknownst to Eve, it turns out that the messages differ only in the 21st byte of the two messages but are otherwise identical.

Yes, Alice screwed up. But how badly? For each possibility, select all which apply.

(a) If Alice used AES-ECB (Electronic Code Book), Eve is able to determine which of the following about $M_2$:

- [ ] That $M_2$ is exactly 120B long
- [ ] That $M_2$ is less than 129B long but not the exact length
- [ ] The entire plaintext for $M_2$
- [ ] The plaintext for only the first two blocks of $M_2$
- [ ] The entire plaintext for $M_2$ except for the 2nd block
- [ ] The plaintext for only the first block of $M_2$
Problem 9  *Screwups in Inserting an IV*  

Alice encrypts two messages, $M_1$ and $M_2$ using the same IV/nonce and a deterministic padding scheme (when appropriate for the particular mode) using AES (a 128b block cipher). Eve, the Eavesdropper, knows the plaintext of $M_1$, that each block of $M_1$ is different, that $M_1$ is 120 bytes, and that Alice never sends any bytes she doesn’t have to. Unbeknownst to Eve, it turns out that the messages differ only in the 21st byte of the two messages but are otherwise identical.

Yes, Alice screwed up. But how badly? For each possibility, select *all* which apply.

(b) If Alice used AES-CTR (Counter), Eve is able to determine which of the following about $M_2$:

- [ ] That $M_2$ is exactly 120B long
- [ ] That $M_2$ is less than 129B long but not the exact length
- [ ] The entire plaintext for $M_2$
- [ ] The plaintext for only the first two blocks of $M_2$
- [ ] The entire plaintext for $M_2$ except for the 2nd block
- [ ] The plaintext for only the first block of $M_2$
Recall CTR: Encryption

Enc(K, plaintext):

- If \( n \) is the block size of the block cipher, split the plaintext in blocks of size \( n \): \( P_1, P_2, P_3, \ldots \)
- Choose a random nonce
- Now compute:

\[
\text{(Nonce = Same as IV)}
\]

Important that nonce does not repeat across different encryptions (choose it at random from large space)

The final ciphertext is \((\text{nonce}, C_1, C_2, C_3)\)
Problem 9  *Screwups in Inserting an IV*  

Alice encrypts two messages, \( M_1 \) and \( M_2 \) using the same IV/nonce and a deterministic padding scheme (when appropriate for the particular mode) using AES (a 128b block cipher). Eve, the Eavesdropper, knows the plaintext of \( M_1 \), that each block of \( M_1 \) is different, that \( M_1 \) is 120 bytes, and that Alice never sends any bytes she doesn’t have to. Unbeknownst to Eve, it turns out that the messages differ only in the 21st byte of the two messages but are otherwise identical.

Yes, Alice screwed up. But how badly? For each possibility, select *all* which apply.

(b) If Alice used AES-CTR (Counter), Eve is able to determine which of the following about \( M_2 \):

- [ ] That \( M_2 \) is exactly 120B long

- [ ] The entire plaintext for \( M_2 \)

- [ ] The entire plaintext for \( M_2 \) except for the 2nd block

- [ ] That \( M_2 \) is less than 129B long but not the exact length

- [ ] The plaintext for only the first two blocks of \( M_2 \)

- [ ] The plaintext for only the first block of \( M_2 \)
Problem 9  Screwups in Inserting an IV  

Alice encrypts two messages, \( M_1 \) and \( M_2 \) using the same IV/nonce and a deterministic padding scheme (when appropriate for the particular mode) using AES (a 128b block cipher). Eve, the Eavesdropper, knows the plaintext of \( M_1 \), that each block of \( M_1 \) is different, that \( M_1 \) is 120 bytes, and that Alice never sends any bytes she doesn’t have to. Unbeknownst to Eve, it turns out that the messages differ only in the 21st byte of the two messages but are otherwise identical.

Yes, Alice screwed up. But how badly? For each possibility, select all which apply.

(b) If Alice used AES-CTR (Counter), Eve is able to determine which of the following about \( M_2 \):

- [ ] That \( M_2 \) is exactly 120B long
- [x] That \( M_2 \) is less than 129B long but not the exact length
- [ ] The entire plaintext for \( M_2 \)
- [ ] The plaintext for only the first two blocks of \( M_2 \)
- [ ] The entire plaintext for \( M_2 \) except for the 2nd block
- [x] The plaintext for only the first block of \( M_2 \)
Problem 9  *Screwups in Inserting an IV* (15 points)

Alice encrypts two messages, $M_1$ and $M_2$ using the same IV/nonce and a deterministic padding scheme (when appropriate for the particular mode) using AES (a 128b block cipher). Eve, the Eavesdropper, knows the plaintext of $M_1$, that each block of $M_1$ is different, that $M_1$ is 120 bytes, and that Alice never sends any bytes she doesn’t have to. Unbeknownst to Eve, it turns out that the messages differ only in the 21st byte of the two messages but are otherwise identical.

Yes, Alice screwed up. But how badly? For each possibility, select *all* which apply.

(c) If Alice used AES-CBC (Cipher Block Chaining), Eve is able to determine which of the following about $M_2$:

- That $M_2$ is exactly 120B long
- The entire plaintext for $M_2$
- The entire plaintext for $M_2$ except for the 2nd block
- That $M_2$ is less than 129B long but not the exact length
- The plaintext for only the first two blocks of $M_2$
- The plaintext for only the first block of $M_2$
Recall CBC: Encryption

Break message $M$ into $P_1 | P_2 | \ldots | P_m$

Choose a random IV (it may not repeat for messages with same $P_1$, it is not secret and is included in the ciphertext)

\[
\text{Enc}(K, P_1 | P_2 | \ldots | P_m) = (\text{IV}, C_1, C_2, \ldots, C_m)
\]
Problem 9  *Screwups in Inserting an IV*  

Alice encrypts two messages, $M_1$ and $M_2$ using the same IV/nonce and a deterministic padding scheme (when appropriate for the particular mode) using AES (a 128b block cipher). Eve, the Eavesdropper, knows the plaintext of $M_1$, that each block of $M_1$ is different, that $M_1$ is 120 bytes, and that Alice never sends any bytes she doesn’t have to. Unbeknownst to Eve, it turns out that the messages differ only in the 21st byte of the two messages but are otherwise identical.

Yes, Alice screwed up. But how badly? For each possibility, select *all* which apply.

(c) If Alice used AES-CBC (Cipher Block Chaining), Eve is able to determine which of the following about $M_2$:

- □ That $M_2$ is exactly 120B long
- □ That $M_2$ is less than 129B long but not the exact length
- □ The entire plaintext for $M_2$
- □ The plaintext for only the first two blocks of $M_2$
- □ The entire plaintext for $M_2$ except for the 2nd block
- □ The plaintext for only the first block of $M_2$
Problem 9  \textbf{Screwups in Inserting an IV} \hspace{1cm} (15 points)

Alice encrypts two messages, $M_1$ and $M_2$ using the same IV/nonce and a deterministic padding scheme (when appropriate for the particular mode) using AES (a 128b block cipher). Eve, the Eavesdropper, knows the plaintext of $M_1$, that each block of $M_1$ is different, that $M_1$ is 120 bytes, and that Alice never sends any bytes she doesn’t have to. Unbeknownst to Eve, it turns out that the messages differ only in the 21st byte of the two messages but are otherwise identical.

Yes, Alice screwed up. But how badly? For each possibility, select \textit{all} which apply.

(c) If Alice used AES-CBC (Cipher Block Chaining), Eve is able to determine which of the following about $M_2$:

- [ ] That $M_2$ is exactly 120B long
- [ ] That $M_2$ is less than 129B long but not the exact length
- [ ] The entire plaintext for $M_2$
- [ ] The plaintext for only the first two blocks of $M_2$
- [ ] The entire plaintext for $M_2$ except for the 2nd block
- [ ] The plaintext for only the first block of $M_2$
Problem 9  Screwups in Inserting an IV  

Alice encrypts two messages, $M_1$ and $M_2$ using the same IV/nonce and a deterministic padding scheme (when appropriate for the particular mode) using AES (a 128b block cipher). Eve, the Eavesdropper, knows the plaintext of $M_1$, that each block of $M_1$ is different, that $M_1$ is 120 bytes, and that Alice never sends any bytes she doesn’t have to. Unbeknownst to Eve, it turns out that the messages differ only in the 21st byte of the two messages but are otherwise identical.

Yes, Alice screwed up. But how badly? For each possibility, select all which apply.

(d) If Alice used AES-CFB (Ciphertext Feedback), Eve is able to determine which of the following about $M_2$:

- [ ] That $M_2$ is exactly 120B long
- [ ] That $M_2$ is less than 129B long but not the exact length
- [ ] The entire plaintext for $M_2$
- [ ] The plaintext for only the first two blocks of $M_2$
- [ ] The entire plaintext for $M_2$ except for the 2nd block
- [ ] The plaintext for only the first block of $M_2$
AES-CFB

Cipher Feedback (CFB) mode encryption
Problem 9  **Screwups in Inserting an IV**

Alice encrypts two messages, $M_1$ and $M_2$ using the same IV/nonce and a deterministic padding scheme (when appropriate for the particular mode) using AES (a 128b block cipher). Eve, the Eavesdropper, knows the plaintext of $M_1$, that each block of $M_1$ is different, that $M_1$ is 120 bytes, and that Alice never sends any bytes she doesn’t have to. Unbeknownst to Eve, it turns out that the messages differ only in the 21st byte of the two messages but are otherwise identical.

Yes, Alice screwed up. But how badly? For each possibility, select *all* which apply.

(d) If Alice used AES-CFB (Ciphertext Feedback), Eve is able to determine which of the following about $M_2$:

☐ That $M_2$ is exactly 120B long

☐ The entire plaintext for $M_2$

☐ The entire plaintext for $M_2$ except for the 2nd block

☐ That $M_2$ is less than 129B long but not the exact length

☐ The plaintext for only the first two blocks of $M_2$

☐ The plaintext for only the first block of $M_2$
Problem 9  **Screwups in Inserting an IV**  (15 points)

Alice encrypts two messages, $M_1$ and $M_2$ using the same IV/nonce and a deterministic padding scheme (when appropriate for the particular mode) using AES (a 128b block cipher). Eve, the Eavesdropper, knows the plaintext of $M_1$, that each block of $M_1$ is different, that $M_1$ is 120 bytes, and that Alice never sends any bytes she doesn’t have to. Unbeknownst to Eve, it turns out that the messages differ only in the 21st byte of the two messages but are otherwise identical.

Yes, Alice screwed up. But how badly? For each possibility, select all which apply.

(d) If Alice used AES-CFB (Ciphertext Feedback), Eve is able to determine which of the following about $M_2$:

- [ ] That $M_2$ is exactly 120B long
- [ ] The entire plaintext for $M_2$
- [ ] The entire plaintext for $M_2$ except for the 2nd block
- [ ] That $M_2$ is less than 129B long but not the exact length
- [ ] The plaintext for only the first two blocks of $M_2$
- [ ] The plaintext for only the first block of $M_2$

I found the problem statement a bit confusing because it says that Alice uses a deterministic padding but later that she does not send any bytes she does not need to. Technically, with CFB you don't need to pad. If you pad, the attacker cannot figure out the length of the last plaintext block, so it cannot tell precisely the length of $M_2$, other than being less than 129 bytes. If you do not pad, then the attacker can tell exactly the length of $M_2$ from the size of the ciphertext with no need for any association to $M_1$. 

Problem 7  *ElGamal and friends*  

Bob wants his pipes fixed and invites independent plumbers to send him bids for their services (*i.e.*, the fees they charge). Alice is a plumber and wants to submit a bid to Bob. Alice and Bob want to preserve the confidentiality of Alice’s bid, but the communication channel between them is insecure. Therefore, they decide to use the ElGamal public key encryption scheme in order to communicate privately.

Instead of using the traditional version of the ElGamal scheme, Alice and Bob use the following variant. As usual, Bob’s private key is $x$ and his public key is \( PK = (p, g, h) \), where $h = g^x \mod p$. However, to send a message $M$ to Bob, Alice encrypts $M$ as $\text{Enc}_{PK}(M) = (s, t)$, where $s = g^r \mod p$ and $t = g^M \times h^r \mod p$, for a randomly chosen $r$.

(a) Consider two distinct messages $m_1$ and $m_2$. Let $\text{Enc}_{PK}(m_1) = (s_1, t_1)$ and $\text{Enc}_{PK}(m_2) = (s_2, t_2)$. For the given variant of the ElGamal scheme, which of the following is true?

- ( ) \( (s_1 + s_2 \mod p, \quad t_1 + t_2 \mod p) \) is a possible value for $\text{Enc}_{PK}(m_1 + m_2)$.
- ( ) \( (s_1 \times s_2 \mod p, \quad t_1 \times t_2 \mod p) \) is a possible value for $\text{Enc}_{PK}(m_1 + m_2)$.
- ( ) \( (s_1 \times s_2 \mod p, \quad t_1 \times t_2 \mod p) \) is a possible value for $\text{Enc}_{PK}(m_1 \times m_2)$.
- ( ) \( (s_1 + s_2 \mod p, \quad t_1 + t_2 \mod p) \) is a possible value for $\text{Enc}_{PK}(m_1 \times m_2)$.
- ( ) None of these
Problem 7  \textit{ElGamal and friends} (15 points)

Bob wants his pipes fixed and invites independent plumbers to send him bids for their services (i.e., the fees they charge). Alice is a plumber and wants to submit a bid to Bob. Alice and Bob want to preserve the confidentiality of Alice’s bid, but the communication channel between them is insecure. Therefore, they decide to use the ElGamal public key encryption scheme in order to communicate privately.

Instead of using the traditional version of the ElGamal scheme, Alice and Bob use the following variant. As usual, Bob’s private key is $x$ and his public key is $PK = (p, g, h)$, where $h = g^x \mod p$. However, to send a message $M$ to Bob, Alice encrypts $M$ as $Enc_{PK}(M) = (s, t)$, where $s = g^r \mod p$ and $t = g^M \times h^r \mod p$, for a randomly chosen $r$.

(a) Consider two distinct messages $m_1$ and $m_2$. Let $Enc_{PK}(m_1) = (s_1, t_1)$ and $Enc_{PK}(m_2) = (s_2, t_2)$. For the given variant of the ElGamal scheme, which of the following is true?

- $(s_1 + s_2 \mod p, \quad t_1 + t_2 \mod p)$ is a possible value for $Enc_{PK}(m_1 + m_2)$.

- $(s_1 \times s_2 \mod p, \quad t_1 \times t_2 \mod p)$ is a possible value for $Enc_{PK}(m_1 + m_2)$.

- $(s_1 \times s_2 \mod p, \quad t_1 \times t_2 \mod p)$ is a possible value for $Enc_{PK}(m_1 \times m_2)$.

- $(s_1 + s_2 \mod p, \quad t_1 + t_2 \mod p)$ is a possible value for $Enc_{PK}(m_1 \times m_2)$.

- None of these
Problem 7  \textit{ElGamal and friends}  \hspace{1cm} (15 points)

Bob wants his pipes fixed and invites independent plumbers to send him bids for their services (i.e., the fees they charge). Alice is a plumber and wants to submit a bid to Bob. Alice and Bob want to preserve the confidentiality of Alice’s bid, but the communication channel between them is insecure. Therefore, they decide to use the ElGamal public key encryption scheme in order to communicate privately.

Instead of using the traditional version of the ElGamal scheme, Alice and Bob use the following variant. As usual, Bob’s private key is $x$ and his public key is $\text{PK} = (p, g, h)$, where $h = g^x \mod p$. However, to send a message $M$ to Bob, Alice encrypts $M$ as $\text{Enc}_{\text{PK}}(M) = (s, t)$, where $s = g^r \mod p$ and $t = g^M \times h^r \mod p$, for a randomly chosen $r$.

(b) In order to decrypt a ciphertext $(s, t)$, Bob starts by calculating $q = ts^{-x} \mod p$. Assume that the message $M$ is between 0 and 1000. How can Bob recover $M$ from $q$?

\textbf{Solution:} If Bob knows the possible set of messages, then he can pre-compute a lookup table for values of $q = g^M \mod p$.

(c) Explain why Bob cannot efficiently recover $M$ from $q$ if $M$ is randomly chosen such that $0 \leq M < p$.

\textbf{Solution:} Requires solving the discrete log $\mod p$, which is thought to be computationally hard.