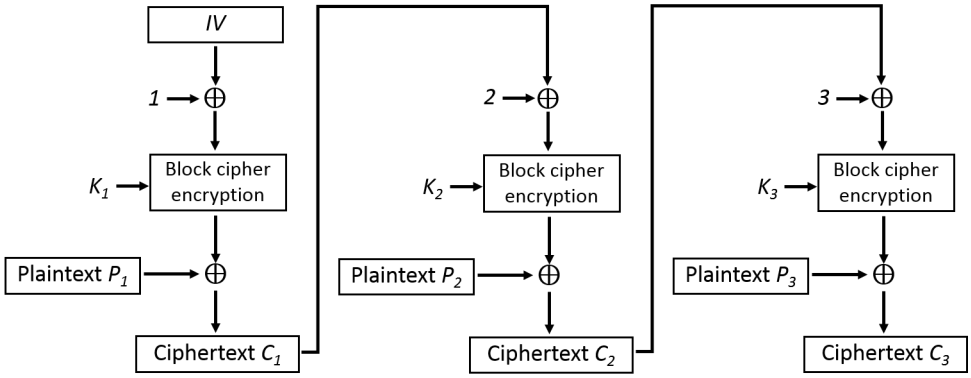
Midterm Review - Symmetric Cryptography

Question 1 ***Socially Distanced Cipher*** **(18 min)**

Bob and Alice want to plan a social distancing picnic, but don't want to invite Eve because she hasn't been wearing a mask in public. They decide to send messages using a new block cipher chaining mode, AES-SDC (Socially Distanced Cipher). Note that AES-SDC requires a different key for each block of the message.

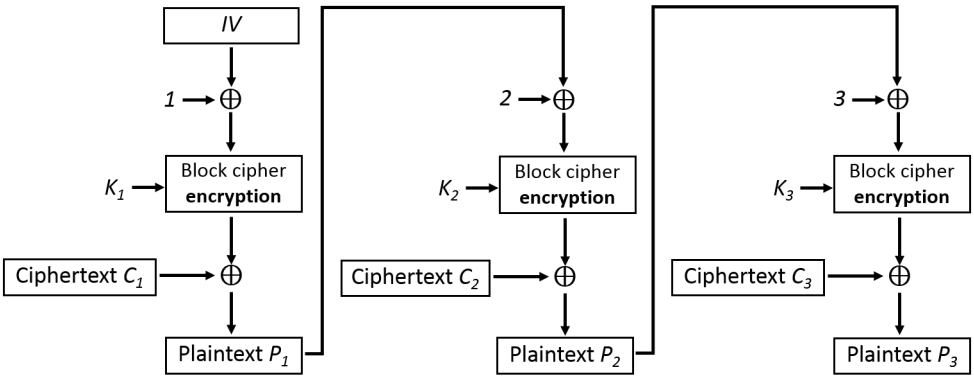
$$C_0 = IV$$

$$C_i = E_{k_i}(C_{i-1} \oplus i) \oplus P_i$$

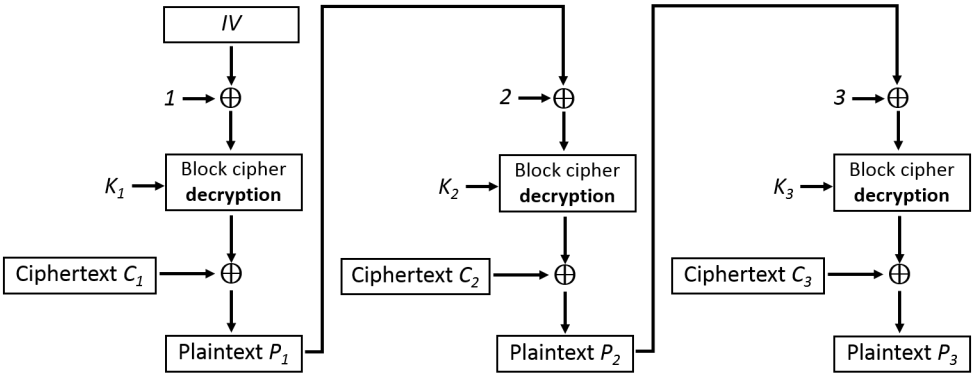


Q1.1 (3 points) Which of the following is the correct decryption expression/diagram for AES-SDC?

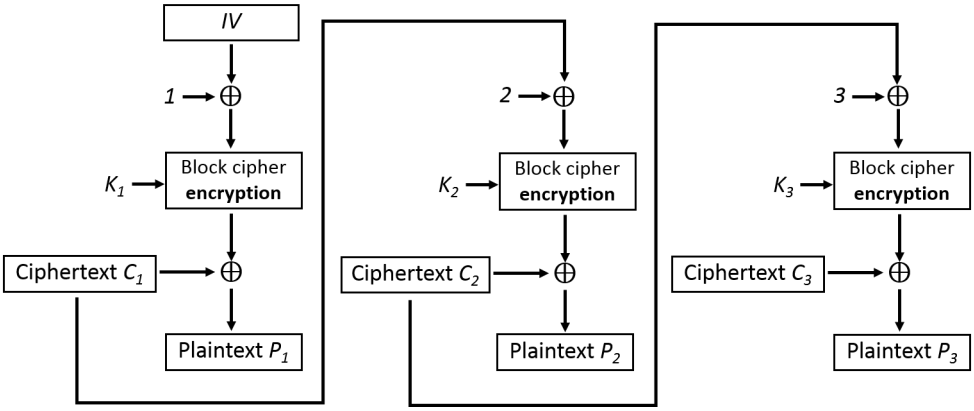
◯ (A) $P_i = E_{k_i}(P_{i-1} \oplus i) \oplus C_i$



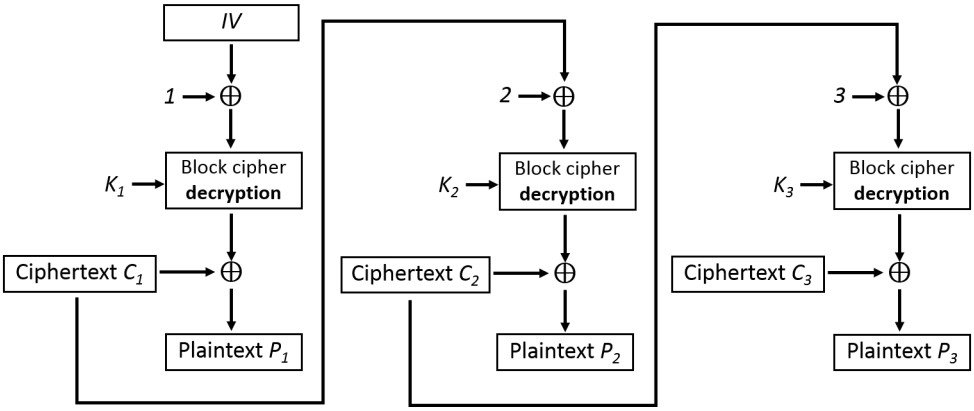
◯ (B) $P_i = D_{k_i}(P_{i-1} \oplus i) \oplus C_i$



◯ (C) $P_i = E_{k_i}(C_{i-1} \oplus i) \oplus C_i$



◯ (D) $P_i = D_{k_i}(C_{i-1} \oplus i) \oplus C_i$



◯ (E) ——

◯ (F) ——

Q1.2 (3 points) Select all true statements about this encryption scheme.

Hint: The cipher mode you saw in Homework 2, $C_i = E_k(C_{i-1}) \oplus P_i$, is IND-CPA secure.

☐ (G) Encryption can be parallelized

☐ (H) Decryption can be parallelized

☐ (I) It is IND-CPA secure

☐ (J) None of the above

☐ (K) —

☐ (L) —

Suppose Alice loses some of her shared keys with Bob. Alice wants to encrypt an n-block message using AES-SDC. For each scenario below, determine which blocks Alice can still encrypt.

Q1.3 (3 points) Alice has all the keys except k_4 and k_5.

◯ (A) Alice can encrypt all parts of her message except P_4 and P_5

◯ (B) Alice can encrypt P_1, P_2 and P_3 only.

◯ (C) Alice can encrypt the entire message

◯ (D) Alice cannot encrypt any block of the message

◯ (E) None of the above

◯ (F) —

Now, suppose Alice now has all the keys, and Alice sends a n-block message to Bob. Eve learns some keys and some blocks of ciphertext. For each scenario below, determine which blocks Eve can decrypt.

Q1.4 (3 points) Eve learns the IV, ciphertext blocks C_5 and C_6, and key k_5.

◯ (G) Eve can decrypt C_5 only

◯ (H) Eve can decrypt C_5 and C_6 only

◯ (I) Eve can decrypt all messages intercepted

◯ (J) Eve cannot decrypt any intercepted messages

◯ (K) None of the above

◯ (L) —

Q1.5 (3 points) Eve learns the IV, ciphertext blocks C_2, C_3, and C_5, and keys k_2, k_3, and k_5.

◯ (A) Eve can decrypt C_3 and C_5 only

◯ (B) Eve can decrypt C_2, C_3, C_5 only

◯ (C) Eve can decrypt C_2, C_3, C_4, C_5 only

◯ (D) Eve can decrypt C_3 only

◯ (E) Eve cannot decrypt any intercepted messages

◯ (F) None of the above

Q1.6 (3 points) Bob receives all the keys and ciphertext blocks C_1 through C_n, but C_3 is corrupted. Which plaintext blocks can Bob successfully decrypt?

◯ (G) Bob can successfully decrypt all blocks except C_3

◯ (H) Bob can successfully decrypt all blocks except C_4

◯ (I) Bob can successfully decrypt all blocks except C_1, C_2, C_3

◯ (J) Bob can successfully decrypt all blocks except C_3 and C_4

◯ (K) Bob cannot successfully decrypt any of the blocks

◯ (L) None of the above

Question 2 ***MAC Madness*** **(18 min)**

Evan wants to store a list of every CS161 student's firstname and lastname, but he is afraid Mallory will tamper with his list.

Evan is considering adding a cryptographic value to each record to ensure its integrity. For each scheme, determine what Mallory can do without being detected.

Assume MAC is a secure MAC, H is a cryptographic hash, and Mallory does not know Evan's secret key k. Assume that firstname and lastname are all lowercase and alphabetic (no numbers or special characters), and concatenation does not add any delimiter (e.g. a space or tab), so nick‖weaver = nickweaver.

Q2.1 (3 points) H(firstname‖lastname)

- ◯ (A) Mallory can modify a record to be a value of her choosing
- ◯ (B) Mallory can modify a record to be a specific value (not necessarily of her choosing)
- ◯ (C) Mallory cannot modify a record without being detected
- ◯ (D) —
- ◯ (E) —
- ◯ (F) —

Q2.2 (3 points) MAC(k, firstname‖lastname)

Hint: Can you think of two different records that would have the same MAC?

- ◯ (G) Mallory can modify a record to be a value of her choosing
- ◯ (H) Mallory can modify a record to be a specific value (not necessarily of her choosing)
- ◯ (I) Mallory cannot modify a record without being detected
- ◯ (J) —
- ◯ (K) —
- ◯ (L) —

Q2.3 (3 points) MAC(k, firstname‖"-"‖lastname), where "-" is a hyphen character.

- ◯ (A) Mallory can modify a record to be a value of her choosing
- ◯ (B) Mallory can modify a record to be a specific value (not necessarily of her choosing)
- ◯ (C) Mallory cannot modify a record without being detected

◯ (D) —

◯ (E) —

◯ (F) —

Q2.4 (3 points) $\mathsf{MAC}(k, \mathsf{H}(\mathsf{firstname})\|\mathsf{H}(\mathsf{lastname}))$

◯ (G) Mallory can modify a record to be a value of her choosing

◯ (H) Mallory can modify a record to be a specific value (not necessarily of her choosing)

◯ (I) Mallory cannot modify a record without being detected

◯ (J) —

◯ (K) —

◯ (L) —

Q2.5 (3 points) $\mathsf{MAC}(k, \mathsf{firstname})\|\mathsf{MAC}(k, \mathsf{lastname})$

◯ (A) Mallory can modify a record to be a value of her choosing

◯ (B) Mallory can modify a record to be a specific value (not necessarily of her choosing)

◯ (C) Mallory cannot modify a record without being detected

◯ (D) —

◯ (E) —

◯ (F) —

Q2.6 (3 points) Which of Evan's schemes guarantee confidentiality on his records?

◯ (G) All 5 schemes

◯ (H) Only the schemes with a MAC

◯ (I) Only the schemes with a hash

◯ (J) None of the schemes

◯ (K) —

◯ (L) —