Symmetric Cryptography

Question 1 ***True/false***

Q1.1 TRUE or FALSE: Using $H(x) = \text{SHA256}(x)$, where x is a message, forms a secure message authentication code.

○ TRUE ● FALSE

Solution: False. There is no key here so anyone can forge a valid MAC.

Q1.2 TRUE or FALSE: Encrypting a message with AES-CBC mode and a random IV is IND-CPA secure.

● TRUE ○ FALSE

Solution: True. This is proper usage of AES-CBC, and as shown in lecture, AES-CBC is IND-CPA secure if properly used.

Q1.3 TRUE or FALSE: Suppose that in an IND-CPA game for some encryption scheme, there is an attacker who finds a way to guess the random bit correctly with probability 0.4. The scheme could still be IND-CPA.

○ TRUE ● FALSE

Solution: False. There is another attacker, the one that makes the opposite guess every time; this attacker has a way to guess the random bit with probability 0.6, which wins the IND-CPA game.

Q1.4 TRUE or FALSE: If Bob uses the authenticate-then-encrypt paradigm, the integrity of his plaintext is guaranteed.

● TRUE ○ FALSE

Solution: True. Authenticate-then-encrypt guarantees integrity for the plaintext, just not the ciphertext.

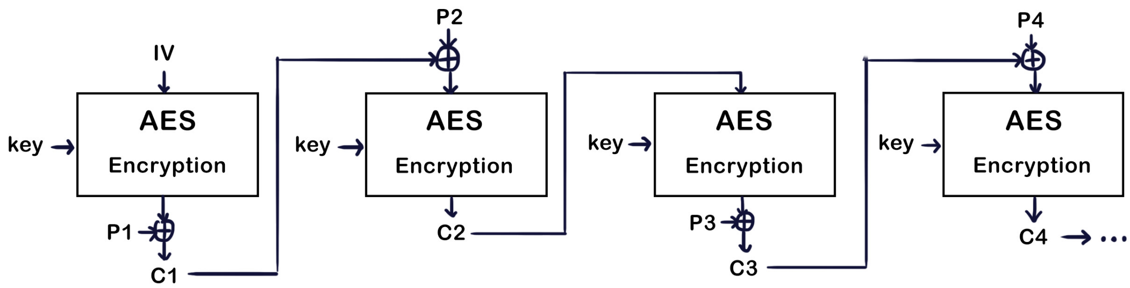
Q1.5 TRUE or FALSE: A hash function must be collision-resistant to be considered safe for password hashing.

○ TRUE ● FALSE

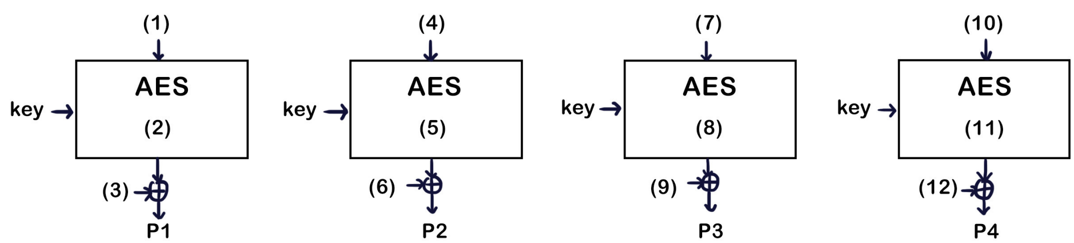
Solution: False. Only the one-way property is needed. Collisions are okay as long as one cannot find a preimage for a given function value.

Question 2 ***EvanBot's Last Creation***

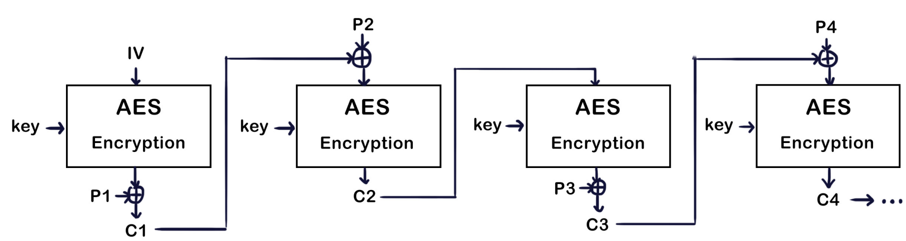
Inspired by different AES modes of operation, EvanBot creates an encryption scheme that combines two existing modes of operation and names it AES-DMO (Dual Mode Operation). Provided below is an encryption schematic of AES-DMO.

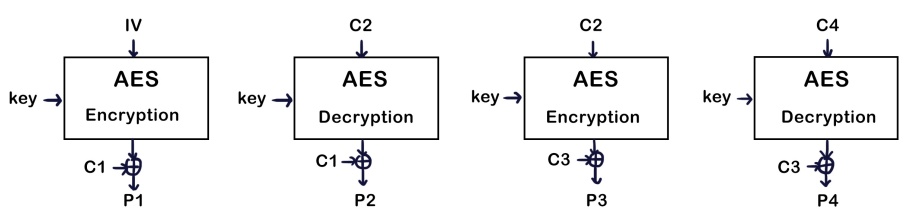


Q2.1 Fill in the numbered blanks for this incomplete decryption schematic of AES-DMO.



Solution:





Q2.2 Select all true statements about AES-DMO.

☐ (G) Encryption can be parallelized

■ (H) Decryption can be parallelized

■ (I) AES-DMO is IND-CPA secure

☐ (J) None of the above

☐ (K) ——

Solution: The diagram for encryption has a feedback from one block to the next, whereas the diagram for decryption has no such feedback. This makes decryption parallelizeable but not encryption.

DMO is IND-CPA because each block is either AES-CBC or AES-CFB, both of which are IND-CPA. You can do a proof by induction: C1 is secure since it's the first block of AES-CFB, and each subsequent block is AES-CFB or AES-CBC where the feedback from the previous block (ciphertext) is IND-CPA, in effect a random number.

Question 3

Alice comes up with a couple of schemes to securely send messages to Bob. Assume that Bob and Alice have known RSA public keys.

For this question, Enc denotes AES-CBC encryption, H denotes a collision-resistant hash function, $||$ denotes concatenation, and $\bigoplus$ denotes bitwise XOR.

Consider each scheme below independently and select whether each one guarantees confidentiality, integrity, and authenticity in the face of a MITM.

Q3.1 Alice and Bob share two symmetric keys k_1 and k_2. Alice sends over the pair $[Enc(k_1, Enc(k_2, m)), Enc(k_2, m)]$.

■ (A) Confidentiality
□ (B) Integrity
□ (C) Authenticity
□ (D) None of the above
□ (E) ——
□ (F) ——

Solution: Note that Enc denotes AES-CBC, not AES-EMAC, so we can only provide confidentiality. An attacker can forge a pair $[Enc(k1, c1), c1]$ given $[Enc(k1, c1||c2), c1||c2]$.

Q3.2 Alice and Bob share a symmetric key k, have agreed on a PRNG, and implement a stream cipher as follows: they use the key k to seed the PRNG and use the PRNG to generate message-length codes as a one-time pad every time they send/receive a message. Alice sends the pair $[m \bigoplus \text{code}, HMAC(k, m \bigoplus \text{code})]$.

■ (G) Confidentiality
■ (H) Integrity
■ (I) Authenticity
□ (J) None of the above
□ (K) ——
□ (L) ——

Solution: This stream cipher scheme has confidentiality since the attacker has no way of coming up with the pseudorandomly generated one-time pads. $HMAC$ provides the integrity and authentication.

Q3.3 Alice and Bob share a symmetric key k. Alice sends over the pair $[Enc(k, m), H(Enc(k, m))]$.

■ (A) Confidentiality
□ (B) Integrity
□ (C) Authenticity
□ (D) None of the above
□ (E) ——
□ (F) ——

Solution: Public hash functions alone do not provide integrity or authentication. Anyone can forge a pair $c, H(c)$, which will pass the integrity check and can be decrypted.

Q3.4 Alice and Bob share a symmetric key k. Alice sends over the pair $[Enc(k, m), H(k||Enc(k, m))]$.

■ (G) Confidentiality

☐ (H) Integrity

☐ (I) Authenticity

☐ (J) None of the above

☐ (K) ——

☐ (L) ——

Solution: $H(k||Enc(k, m))$ is not a valid substitute for $HMAC$ because it is vulnerable to a length extension attack.

Question 4

EvanBot has decided to switch career paths and pursue creating new cryptographic hash functions. EvanBot proposes two new hash functions, E and B:

$$E(x) = H(x_1 x_2 \dots x_{M-1})$$
$$B(x) = H(x_1 x_2 \dots x_M || 0)$$

where H is a preimage-resistant and collision-resistant hash function, $x = x_1 x_2 \dots x_M$, $x_i \in \{0, 1\}$ and $||$ denotes concatenation.

In other words, $E(x)$ calls H with the last bit of x removed, and $B(x)$ calls H with a 0 bit appended to x.

Q4.1 Is $E(x)$ preimage-resistant? Provide a counter-example if it is not.

- ● (A) Yes
- ○ (B) No
- ○ (C) —
- ○ (D) —
- ○ (E) —
- ○ (F) —

Counterexample:

Q4.2 Is $E(x)$ collision-resistant? Provide a counter-example if it is not.

- ○ (G) Yes
- ● (H) No
- ○ (I) —
- ○ (J) —
- ○ (K) —
- ○ (L) —

Counterexample:

Solution: $E(x)$ is preimage-resistant. Suppose not, i.e., given $E(x)$ we could find an x' such that $E(x) = E(x')$. We will argue this means that H is not preimage-resistant, either. Suppose we are given $H(y)$. Let $x = y0$, so that $E(x) = H(y)$. By assumption, we can find x' such that $E(x) = E(x')$. Let $y' = x'_1 \cdots x'_{M-1}$. Then it follows that $H(y) = E(x) = E(x') = H(y')$, so given $H(y)$ we can find y' such that $H(y) = H(y')$. This implies that H is not preimage resistant. That is a contradiction, so our assumption that E was not preimage-resistant must have been wrong.

$E(x)$ is not collision-resistant. Counter example: $E(1 \cdots 010) = E(1 \cdots 011)$, Q4.3 Is $B(x)$ preimage-resistant? Provide a counter-example if it is not.

● (A) Yes ○ (C) —— ○ (E) ——

○ (B) No ○ (D) —— ○ (F) ——

Counterexample:

Q4.4 Is $B(x)$ collision-resistant? Provide a counter-example if it is not.

● (G) Yes ○ (I) —— ○ (K) ——

○ (H) No ○ (J) —— ○ (L) ——

Counterexample:

Solution:

$B(x)$ is preimage resistant, using the same reasoning as $E(x)$. (If there is an attack B's preimage-resistance, then we can construct an attack against H's preimage-resistance that succeeds half as often, which is often enough to show that H is not preimage-resistant — but we were promised that H is preimage-resistant, so it follows that B must be preimage-resistant, too.)

$B(x)$ is collision-resistant. If $B(x)$ was not collision resistant, then we can find $x \neq y$ such that $B(x) = B(y)$. This can be rewritten as $H(x\|0) = H(y\|0)$. Letting $x' = x'\|0$ and $y' = y'\|0$, this means we found $x' \neq y'$ such that $H(x') = H(y')$, which proves that $H(\cdot)$ is not collision-resistant, which is a contradiction. Thus $B(x)$ must be collision-resistant.