Peyrin & Ryan
Summer 2020

CS 161
Computer Security

Final Review

Symmetric Cryptography

Question 1 ***True/false***

Q1.1 True or False: Using $H(x)$ = SHA256(x), where x is a message, forms a secure message authentication code.

○ True ○ False

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

○ True ○ False

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

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

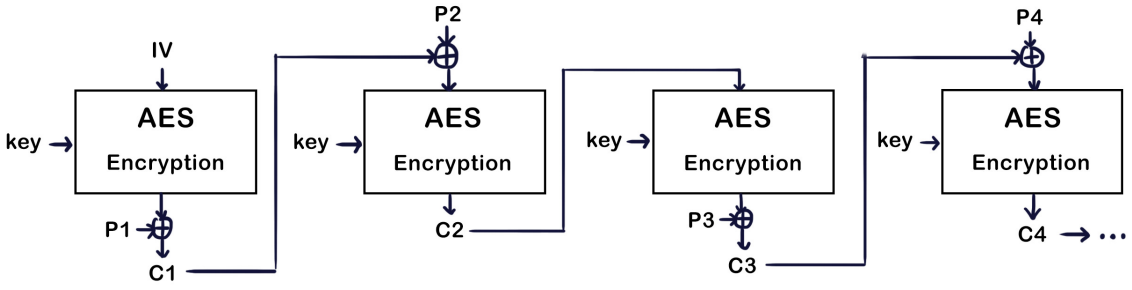
○ True ○ False

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

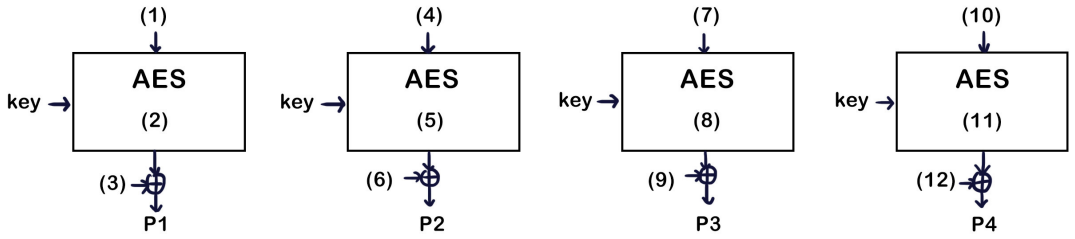
○ True ○ False

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.



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) ——

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 ☐ (C) Authenticity ☐ (E) ——

☐ (B) Integrity ☐ (D) None of the above ☐ (F) ——

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 ☐ (I) Authenticity ☐ (K) ——

☐ (H) Integrity ☐ (J) None of the above ☐ (L) ——

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

☐ (A) Confidentiality ☐ (C) Authenticity ☐ (E) ——

☐ (B) Integrity ☐ (D) None of the above ☐ (F) ——

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 ☐ (I) Authenticity ☐ (K) ——

☐ (H) Integrity ☐ (J) None of the above ☐ (L) ——

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:

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

where H is a preimage-resistant and collision-resistant hash function, $x = x_1 x_2 \ldots x_M$, $x_i \in \{0, 1\}$ 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 ◯ (C) — ◯ (E) —

◯ (B) No ◯ (D) — ◯ (F) —

Counterexample:

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

◯ (G) Yes ◯ (I) — ◯ (K) —

◯ (H) No ◯ (J) — ◯ (L) —

Counterexample:

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: