Quiz-I Cryptography Max Time 10 Mins

Max Marks 10 ME Information Security

All questions carry Single Mark and have single answer.

Q1. Kerckhoffs' principle states that

A) Only the key should be kept secret, but the methods or algorithms used to encrypt and decrypt should be publically known.
B) Keys as well as the scheme of encryption containing the cipher methods should be kept secret.
C) END and DEC algorithms should be kept secret and it is not risky even if key falls into the enemy's hands

Q2. Adversary learns one or more pairs of plaintexts/cipher texts encrypted under the same key. The aim of the adversary is then to determine the plaintext that was encrypted to give known cipher text. This scheme is called

A) Cipher Text Only attack
B) Known Plain Text Attack
C) Chosen Plain text attack
D) Chosen Cypher text attack

Q3. 2nd and Third Frequent letters in a given English Literature are

A) T and A B) E and A C) T and E D) I and A

Q4. You are given a message (m) and its OTP encryption (c). Can you compute the OTP key from m and c ?

A) No, I cannot compute the key.
B) Yes, the key is $k = m \oplus c$
C) I can only compute half the bits of the key.
D) Yes, the key is $k = m \oplus m$.

Q5. Can a stream cipher have perfect secrecy?

A) Yes, if the PRG is really "secure"
B) No, there are no ciphers with perfect secrecy
C) Yes, every cipher has perfect secrecy
D) No, since the key is shorter than the message

Q6. Suppose $G:K \longrightarrow \{0,1\}^n$ is such that for all k: XOR(G(k)) = 1 Is G predictable.

A) Yes, given the first bit I can predict the second
B) No, G is unpredictable
C) Yes, given the first (n-1) bits I can predict the n'th bit
D) It depends

Q7. Let $G:K \longrightarrow \{0,1\}^n$ be a PRG such that from the last n/2 bits of G(k) it is easy to compute the first n/2 bits. Is G predictable for some $i \in \{0, \ldots, n-1\}$?

A) Yes
B) No

Q8. Let $F: K \times X \rightarrow \{0,1\}^{128}$ be a secure PRF. Is the following G a secure PRF?

G(k, x) = 0^{128} if x=0 and F(k,x) otherwise

A) No, it is easy to distinguish G from a random function
B) Yes, an attack on G would also break F
C) It depends on F

Q9. What are the possible key sizes of AES?

A) 128, 192, 256
B) 128, 256, 512
C) 64, 128, 256
D) 128,192,246

Q10. Let I = (S,V) be a MAC. Suppose an attacker is able to find $m_0 \neq m_1$ such that $S(k, m_0) = S(k, m_1)$ for ½ of the keys k in K Can this MAC be secure?

A) Yes, the attacker cannot generate a valid tag for m_0 or m_1
B) No, this MAC can be broken using a chosen msg attack
C) It depends on the details of the MAC