CS2107 Mid-Term Quiz/Exam: Last Year's Questions

Instruction: Choose the ***best answer***, and circle/cross the corresponding letter choice below.

1. In our course's convention, Mallory is an entity who ______________________________ the transmitted messages.
(***Notes***: "Sniff" means eavesdrop on other people's conversations.
"Spoof" means actively introduce/inject forged messages.)

a) can sniff, but can't spoof, can't modify, and can't drop

b) can sniff, can spoof, but can't modify, and can't drop

c) can spoof, can modify, can drop, but cannot sniff

d) can sniff, can spoof, can modify, and can drop

2. Which statement below is ***incorrect*** about IV as used in encryption?

a) IV has to be kept secret from Eve and Mallory

b) It stands for "Initialization Vector" or "Initial Value"

c) IV is used in stream cipher so that the generator can be non-deterministic/ probabilistic in generating the keystream (long bit sequence)

d) IV is used in modes-of-operation such as CBC and CTR so that the encryption becomes non-deterministic/probabilistic.

3. Shift cipher is a type of substitution cipher. In shift cipher, each letter in the plaintext is "shifted" a certain number of places (i.e. the "shift distance") down the alphabet. For example, with a shift of 1, a would be replaced by b, b would become c, and so on. If we assume the set of symbols U={'a', 'b', 'c', …, 'z', '_'} as the alphabet like in our lecture notes, what is the ***key space size*** of this shift cipher, including a trivial encryption where each letter is mapped to itself?

a) 27!

b) 2^{27}

c) 27

d) $\log_2(27!)$

e) $\log_2(27)$

4. Bob intends to increase the security of his stream cipher. Instead of using just one 16-byte (128-bit) secret key, he now utilizes two 16-byte secret keys: k_1 and k_2. Bob first performs the following XOR operation: $k_1 \oplus k_2$. He then supplies the XOR result as the secret key of the stream cipher. What's the ***key space size*** of Bob's new/modified stream cipher? (**Remark**: Please carefully differentiate between bytes and bits.)

a) 2^{128}

b) 2^{256}

c) 2^{16}

d) 2^{32}

e) 2^{255}

5. Bob likes the number 100, which he views as his lucky number. He wants to use a 100-bit key for a secret-key based encryption he develops. Suppose it takes 1,024 clock cycles to test whether a 100-bit encryption key is correct, when given a 100-bit plaintext and its corresponding ciphertext. How long does it take to exhaustively check **all the keys** using a **4GHz single-core** processor? (**Hint**: For simplicity, you can take 1 year ≈ 2^{25} seconds.
Also note that: 1K = 2^{10}, 1M = 2^{20}, 1G = 2^{30}.)

a) 2^{78} years

b) 2^{32} years

c) 2^{10} years

d) 2^{22} years

e) 2^{53} years

6. Bob uses **One-Time Pad (OTP)** by itself for a secure message communication using random and fresh keys. His plaintexts, however, always start with "From: Bob" string, and this is known by Mallory. Mallory wants to change Bob's intercepted ciphertext so that, when decrypted by the legitimate recipient, the plaintext says "From: Mal" instead. Mallory knows that she should XOR the 7th character corresponding to 'B' so that the recovered plaintext becomes 'M' instead. What XOR operation should that be?
(**Note**: Suppose the two relevant characters are encoded using their following ASCII-based binary strings: 'B' → 0100 0010, 'M' → 0100 1101.)

a) XOR the target ciphertext's character with 0100 0010

b) XOR the target ciphertext's character with 0100 1101

c) XOR the target ciphertext's character with 0000 1111

d) XOR the target ciphertext's character with 1111 0000

e) XOR the target ciphertext's character with 1001 0110

7. The following cryptography primitive/operation can provide both integrity and authenticity, but ***not*** non-repudiation:

a) Encryption

b) Hash

c) MAC

d) Digital signature

8. The following pieces of information are contained inside an end-entity's certificate, ***except***:

a) The owner/subject of the certificate

b) The public key of the issuer

c) The issuer name

d) Validity period

9. Alice wants to select a **case sensitive alphanumeric (a-z, A-Z, 0-9)** password for an **online banking login page**. She wants to follow the recommendation in RFC 4086. Which is the shortest length that meets the security recommendation as discussed in the lecture?

a) 4

b) 5

c) 7

d) 9

e) 10

10. Suppose now Alice wants to set a password for her home WiFi access point (using WPA2-PSK). Note that, in this case, **a cryptographic key is to be generated** from the password. Alice wants to follow the recommendation in RFC 4086 and also meet the NIST recommendation. Which is the **shortest case-sensitive**

alphanumeric password length that meets the requirement discussed in the lecture?

a) 8

b) 12

c) 16

d) 22

e) 32

11. Which statement about Bob's digital signature below is ***incorrect***?

a) Bob uses his private key to sign

b) The receiver of Bob's signed message uses Bob's public key to verify the signature

c) RSA employs the hash-and-encrypt approach in generating a digital signature

d) Generally, MAC algorithm (e.g. HMAC) is much faster than signature algorithm (e.g. DSA)

e) It is safe for RSA signing operation to employ MD5

12. In RSA, which task below is computationally difficult?
(Note on the notation used: n is the RSA modulus; p and q are both the modulus' prime factors):

a) Given p and q, compute n

b) Given n and p, compute q

c) Given n and q, compute p

d) Given p and q, compute $\phi(n)$

e) Given n, compute $\phi(n)$

~~~ END OF PAPER ~~~