CS2107 In-Lecture Quiz 2 - Answers
28 September 2022

1. [0.5 mark] The following cryptography primitive/operation can provide both integrity and authenticity, but ***not*** non-repudiation:

a) Encryption

b) Hash

c) MAC

d) Digital signature

2. [0.5 mark] 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

3. [1 mark] 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

4. [1 mark] 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

5. [1 mark] 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

6. [1 mark] 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 $\phi(n)$