IoT Security and Privacy

Assignment 1 - Introduction to Cryto
(10 points)

Questions (Refer to Computer Networking a Top-Down Approach 6th Edition – Chapter 8 if necessary to answer the questions below):

1. What are the differences between message confidentiality and message integrity? Can you have confidentiality without integrity? Can you have integrity without confidentiality? Justify your answer. (3 points)

Message confidentiality is when the sender and receiver are the only ones able to understand the contents of the message. Message integrity is when the contents of the message are not changed by a third party. You can have confidentiality without integrity if the attacker cannot understand the original message before changing it. You can have integrity without confidentiality if the contents are not changed and the attacker can understand the original message.

2. Suppose n = 10,000, a = 10,023, and b = 10,004. Use an identity of modular arithmetic to calculate in your head (a • b) mod n. (1 point)

10,023 mod 10,000 = 23
10,004 mod 10,000 = 4
23 * 4 = 92
92 mod 10,000 = 92

3. Consider RSA with p = 7 and q = 17.
a. What are n and z? (1 point)

p * q = 7 * 17 = 119 = n
(p-1)(q-1) = 6 * 16 = 96 = z

b. Let e be 5. Why is this an acceptable choice for e? (1 point)
Because 5 is prime

c. Find d such that de = 1 (mod z). (1 point)

d(5) = 1 mod 96

d(5) = 1
d = 1/5

d. Encrypt the message m = 8 using the key (n, e). Let c denote the corresponding ciphertext. Show all work. (1 points)

m = 8
m^e = 8 ^ 5 = 32,768
c = m^e mod n = 32,768 mod 119 = 43 = c

4. Reliably publishing public keys is a grand challenge. One popular way is the use of certificates created by a Certificate Authority (CA) such as DigiCert. To get a certificate from a CA, a client provides its public key, identity (such as IP and/or email) and other info to the CA, which rigidly verifies all the information. The CA then provides a certificate to the client. The certificate includes the information provided by the client (denoted as *M*), other information (denoted as *M'*) including the certificate expiration date, and digital signature of *M*|*M'* (where | means concatenation). Assume CA has a public/private key pair (e_{ca}, d_{ca}). The certificate looks like this: (*M*, *M'*), d_{ca}(H(*M*|*M'*)). Actually when people buy computers, public keys of CAs are shipped with the operating system (e.g., Windows/Linux/MacOS/iOS/Andorid/etc.) in the format of certificate too. That is, e_{ca} is already in the OS and trusted.

Question: When a client accesses a web server, the web server sends its certificate signed with a CA's private key d_{ca} to the client. Please explain how the client may verify the certificate is valid and thus gets the web serve's public key. (2 points)

There are multiple way to verify the certificate. One way it to check if its expired or not. You can also check the certificate's hash to the hash of the certificate's public key. Than, the client verifies the certificate by using the certificate's public key and getting the web server's public key.