CENG471 – CRYPTOGRAPHY

Midterm-2 – 2019 FALL Term – Dec. 17, 2019

Student No & Name: ______________________________

Q.1 (25 points)

a) (15 points) We do not confuse confidentiality with authentication terms and concepts. Please use these words with correct meanings in the following story:

"Whether or not a person is allowed access to something is part of the ______________ and authorization processes. An analogy: You are throwing a party. Because your house got trashed the last time, you want to ensure that only people who are invited attend. That is ______________, because you decided up front who would be invited. When the people come, they have to present an invitation to the doorman. That is ______________, because each guest had to show proof that they are who they claim to be. In general, ________________ is planned in advance while ________________ happens as a user attempts to access a system.

Answer:

"Whether or not a person is allowed access to something is part of the authentication and authorization processes. An analogy: You are throwing a party. Because your house got trashed the last time, you want to ensure that only people who are invited attend. That is confidentiality, because you decided up front who would be invited. When the people come, they have to present an invitation to the doorman. That is authentication, because each guest had to show proof that they are who they claim to be. In general, confidentiality is planned in advance while authentication happens as a user attempts to access a system.

b) (10 points) Please calculate the result value for $\mathbf{7^{43}} \equiv ?\ \boldsymbol{mod\ 41}$.

Answer: $7^{43} = 7^{40}.7^3 mod\ 41$ and from FLT we know that $7^{40} \equiv 1\ mod\ 41$ so $7^3 mod\ 41 = 343\ mod\ 41\ \equiv 15$

Q.2 (25 points) Answer the questions below regarding key generation with Diffie-Hellman and RSA.

a) **(5 points)** Suppose the Diffie-Hellman public values *p* and *g* are 7 and 4, respectively. Compute a legal *y* value.

b) **(5 points)** Suppose your partner's *y* value is 3. What is your shared key?

c) **(5 points)** Suppose that you are computing an RSA key pair. What are *p* and *q* and $\Phi(n)$ for $n = 51$?

d) **(5 points)** Find a legal RSA public key pair for this *p* and *q.*

e) **(5 points)** How many possible values for *e* are there?

Answer:

a) $y = g^x mod\ p$ where *x* could be pretty much any value, I will choose 4. Therefore, $y = 4^4 mod\ 7$ = 256 mod 7 = 4.

b) The shared key z = y^xmodp = 3^4mod 7 = 4.

c) p = 3, q = 17 (or vice versa), and Q(n) = 2 . 16 = 32.

d) A valid e is 5, as it is relatively prime to 32. Given e = 5, d.e mod $\Phi(n)$ = 1, so d can equal 13 (5.13mod32 = 1). Officially, d = (13, 51) and e = (5, 51).

e) Odd numbers less than 32 = 16. Other odds are permissible in general too.

Q.3 (25 points)

a) (5 points) Why should you include a message authentication code (MAC) with a message? What is the difference between a MAC and an HMAC?

Student No & Name: ______________________________

Answer: Provide authenticity and especially integrity. HMAC is a special form of a MAC that prevents extension attacks. HMAC computes $h(K \oplus a \parallel K \oplus b \parallel m)$, where a and b are specified constants. The message itself is only hashed once, and the output hashed again with the key.

b) **(10 points)** Alice's ElGamal public key is $(p, \alpha, \beta) = (17,3,6)$. Bob is confused which of two different ElGamal signatures (without hash) for the message *m = 12* he wrote down is the correct one: one of these possible signatures has appendix *(r, s) = (13, 7),* the other *(r, s) = (12, 8).* Check which of them is the valid signature. $(Hint: v_1 \equiv \beta^r r^s, v_2 \equiv \alpha^m \ mod\ p)$

Answer: Bob has to check $v_1 \equiv v_2 \ mod\ p$ or not. If $(r, s) = (13,7)$, then $v_1 = 6$ and $v_2 = 4$.
In the case $(r, s) = (12,8)$ we have $v_1 \equiv 4 \equiv v_2 \ mod\ 17$, hence only second signature value is correct.

c) **(10 points)** Suppose a second message m' = 7 is signed with signature (r', s') = (12, 15). Find (together with the knowledge from the first part) the secret integer k. $(Hint: In\ the\ ElGamal\ signature\ scheme, s \equiv k^{-1}(m - a.r) mod\ p - 1)$

Answer:

Let $(r, s) = (12,8)$ and $(r', s') = (12,15)$. Since $r = r'$, the same k was used for both signatures. We get;

$$s.k - m \ \equiv -a.r \equiv s'.k - m' \ mod\ p - 1,$$

therefore

$$(s - s').k \equiv m - m' \quad mod\ p - 1$$

that is

$$(-7).k \equiv 5\ mod\ 16$$

Now, $gcd(-7,16) = 1$, and (with the extended Euclidean algorithm) we get,

$$k \equiv (-7)^{-1}.5 \equiv 13\ mod\ 16$$

Q.4) (25 points) In this task, we shall consider the RSA public key (n,e) = (667, 417).

a) **(15 points)** Given that 667 = 23 · 29, find the corresponding RSA private key d.

b) **(10 points)** Explain the basic RSA encryption scheme. Compute the decryption of the message C =2, what is the m?

Answer:

a) n=667=p.q=23.29 ➔ $\Phi(n) = (23 - 1)(29 - 1) = 22.28 = 616$
Public key is given as e = 417. We will use Extended Euclidean Algorithm and its backward steps:

616=1.417+199	= 21.417 – 44.(616 – 417) = 21.417 – 44.616 + 44.417 = **65.417 – 44.616**
417=2.199+19	= 21.(417 – 2.199) – 2.199 = 21.417 – 42.199 – 2.199 = 21.417 – 44.199
199=10.19+9	=19-2(199–10.19)=19 – 2.199 + 20.19 = 21.19 – 2.199
19=2.9+1	1=19–2.9

Student No & Name: ______________________________

So; **1= 65.417 – 44.616 ➔ 1 = 27105 – 27104 The private key is d=65 which is the multiplicative inverse of 417 for modulus 616.**

In basic encryption scheme of RSA; $C=m^e \bmod n$

And basic decryption scheme; $M=C^d \bmod n$

b) For C=2 decryption is: $M=2^{65} \bmod 667$; to calculate the result we can use repeated squaring method:

$2^2= 4 \bmod 667$

$2^4=(2^2)^2= 4^2=16 \bmod 667$

$2^8=(2^4)^2=16^2=256 \bmod 667$

$2^{16}=(2^8)^2=256^2=65536 \bmod 667 = 170$

$2^{32}=(2^{16})^2=170^2=28900 \bmod 667 = 219$

$2^{64}=(2^{32})^2=219^2=47961 \bmod 667= 604$

$2^{65}=2^{64}.2= 604.2 \bmod 667 = 541$; hence m=541.