CIS 3362 Homework #4 - Both Groups

Assigned: Wednesday, November 4, 2015
Due Date: Check Webcourses

Directions: Please complete these questions with no computer programs, except for question 4b. You may use a calculator but please clearly write out all of the set up for your calculations as most of the grade is based on the set up and not the answer itself. Please submit a .pdf file via WebCourses before the due date/time posted there.

1) The input into the DES expansion matrix Ebox is `E02AB943` represented in hexadecimal. What is the output of the Ebox, also expressed in hexadecimal. (Note: Your answer should have 12 hex digits.)

2) If the initial 128-bit AES is represented in hexadecimal is

```
912A8E21 FEFEFEFE ABABABAB 93C7D583
```

Determine W(4), the first 32 bits of the key used in round 1 and represent your answer in hexadecimal.

3) If the input, a, for AES is the following,

3C	07	3C	07
07	4D	3C	07
4D	07	A4	3C
A4	4D	07	3C

What is the resulting state matrix after performing the s-box substitution and row-shift in the first round?

4) What is the prime factorization of the following numbers

(a) 196344000 (b) 12206479 (c) 54074592 (d) 1112431320

5) Determine the following values using the formula for the Euler phi function:

(a) $\varphi(196344000)$ (b) $\varphi(12206479)$ (c) $\varphi(54074592)$ (d) $\varphi(1112431320)$

6) What is the remainder when 37^{129} is divided by 80?

7) Using Fermat's Theorem, determine $171^{182} \bmod 181$.

8) Using Euler's Theorem, determine mod 21^{2025} mod 235.

9) In an RSA scheme, p = 7, q = 13 and e = 5. What is d?

10) In an RSA scheme, p = 11, q = 17 and e = 27. What is d?

11) Alice's public El Gamal keys are p = 23, g = 11, and b = 14. You wish to send Alice the message M = 6. You choose the random value k = 4. What are the two ciphertexts (c_1 and c_2) that you send to Alice when you encrypt your message M(6)?

12) In the Diffie-Hellman Key Exchange, let the public keys be p = 29, g = 8, and the secret keys be a = 6 and b = 7, where a is Alice's secret key and b is Bob's secret key. What value does Alice send Bob? What value does Bob send Alice? What is the secret key they share?

13) Consider a situation where we have three users A, B and C. Let's say that we want four secret keys: One shared by A and B only, another shared by B and C only, a third shared by A and C only, and a fourth shared by all three. The three users decide to modify Diffie-Hellman. All three choose to share a prime, p and a generator g. Then all three choose secret numbers, a, b, and c, respectively. User A calculates g^a mod p, user B calculates g^b mod p and user C calculates g^c mod p. They each send their result to the other two users, who take what they receive and raise it to their secret key mod p. These three calculated results are the pair-wise secret keys between A and B, A and C, and B and C. Then, A sends g^{ab} mod p to C, A sends g^{ac} mod p to B and B sends g^{bc} to A. Each recipient of these messages raises them to the power of their private key mod p. When this is all done, all three users have the shared private key g^{abc} mod p. The key shared between A and B is g^{ab} mod p the key shared between A and C is g^{ac} mod p and the key shared between B and C is g^{bc} mod p.

What is the major flaw in this idea?

14) In a Knapsack Cryptosystem, the private key super-increasing set is {7, 8, 20, 53, 96, 200, 397, 818}. Let the public value u = 1836. Select the private value w = 1645. List the public set of value, in order, that would allow someone to send a message to the person who generated these keys.

15) Consider the Elliptic Curve $E_{29}(2,3)$. Let P = (14, 7) and Q = (26, 17). Calculate both P+Q and 2P.

16) Consider the elliptic curve $y^2 = (x^3 + 10x + 7)$ mod 29. Let the point P be (6, 14) and the point Q be (15, 20), on this curve. Determine the points 2P and P + Q.