Fall 2015 CIS 3362 Homework #4 Solutions (Both Groups)

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.)

Solution

```
Original
1110
0000
0010
1010
1011
1001
0100
0011

Expanded
111100
000000
000101
010101
010111
110010
101000
000111

In Hex: F 0 0 1 5 5 5 F 2 A 0 7 (6 pts, 1/2 pt hex, round down)
```

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 hex.

Solution

```
1) Cyclically shift 93C7D583 to get C7D58393. (1 pts)
2) Using the sbox obtain: C603ECDC. (1 pts)
3) The round constant is r(4) = 2^0 = 01 in hex. (1 pts)
4) XOR r(4) with the first byte: C703ECDC.(1 pts)
Now, compute the following XOR 912A8E21 and C703ECDC:

912A8E21 = 1001 0001 0010 1010 1000 1110 0010 0001
C703ECDC = 1100 0111 0000 0011 1110 1100 1101 1100
           -----------------------------------
XOR        0101 0110 0010 1001 0110 0010 1111 1101 (2 pts)
W(4) = 562962FD.(2 pts)
```

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?

Solution

EB	C5	EB	C5
E3	EB	C5	C5
49	EB	E3	C5
EB	49	E3	C5

Grading: 1 pt all shifts, 4 pts subs - 1 pt per sub

4) What is the prime factorization of the following numbers?

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

Solution
(a) $2^6 3^5 5^3 101^1$ - can use a program or calculator to divide out until we get to 101.
(b) $41^1 297719^1$ - probably need a program for this one
(c) $2^5 3^2 11^1 13^2 101$ - can use a program or calculator to divide out until we get to 101.
(d) $2^3 3^4 5^1 7^4 11^1 13^1$ - can use a program or calculator to divide out until we get to 101.

Grading: 2 pts each, give 1 pt if close but not correct

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

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

Solution
(a) $\varphi(196344000) = \varphi(2^6 3^5 5^3 101^1) = \varphi(2^6)\,\varphi(3^5)\,\varphi(5^3)\,\varphi(101^1)$
$= (2^6 - 2^5)\,(3^5 - 3^4)\,(5^3 - 5^2)(101 - 1) = 51840000$
(b) $\varphi(12206479) = \varphi(41^1 297719^1) = \varphi(41^1)\varphi(297719^1) = (41 - 1)(297719 - 1) = 11908720$

(c) $\varphi(54074592) = \varphi(2^5 3^2 11^1 13^2 101) = \varphi(2^5)\varphi(3^2)\varphi(11^1)\varphi(13^2)\varphi(101^1)$
$= (2^5 - 2^4)\,(3^2 - 3^1)\,(11 - 1)(13^2 - 13^1)(101 - 1) = 14976000$

(d) $\varphi(1112431320) = \varphi(2^3 3^4 5^1 7^4 11^1 13^1) = \varphi(2^3)\varphi(3^4)\varphi(5^1)\varphi(7^4)\varphi(11^1)\varphi(13^1)$
$= (2^3 - 2^2)\,(3^4 - 3^3)\,(5 - 1)(7^4 - 7^3)(11 - 1)(13 - 1) = 213373440$

Grading: 2 pts each, give 1 pt if close but not correct

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

Solution
$\varphi(80) = \varphi((5)(16)) = \varphi(5)\varphi(16) = (5 - 1)(16 - 8) = 32$. (1 pt)

Thus, $37^{32} \equiv 1 \bmod 80$, using Euler's formula since gcd(37, 80) = 1.

$37^{129} \equiv (37^{32})^4(37) \bmod 80$ (1 pts)
$\equiv (1)^4(37) \bmod 80$
$\equiv 37 \bmod 80$ (1 pt)

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

Solution
Since 181 is prime, Fermat's Theorem tells us that $171^{180} \equiv 1 \bmod 181$. (1 pt)

It follows that

$171^{182} \equiv 171^{180} \times 171^2 \equiv 1 \times (-10)^2 \equiv 100 \bmod 181$. (2 pts)

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

Solution
Since gcd(21, 235) = 1, Euler's Theorem applies to this calculation.

First, note that $\varphi(235) = \varphi(5 \times 47) = \varphi(5) \times \varphi(47) = (5 - 1)(47 - 1) = 184$. (1 pt)

Next, note that $2025 = 11 \times 184 + 1$. It follows that $21^{184} \equiv 1 \bmod 235$. (1 pt)

Thus, we have:

$21^{2025} \equiv 21^{11(184) + 1} \equiv (21^{184})^{11}(21^1) \equiv 1^{11}21^1 = 21 \bmod 235$. (1 pt)

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

Solution
n = 7x13 = 91
φ(n) = (7 – 1)(13 – 1) = 72. (2 pts)

ed ≡ 1 mod 72
5d ≡ 1 mod 72

Thus, we must find 5^{-1} mod 72. Use the Extended Euclidean Algorithm:

72 = 14x5 + 2
5 = 2x2 + 1 (2 pts)

5 – 2x2 = 1
5 – 2(72 – 14x5) = 1
5 – 2x72 + 28x5 = 1
29x5 – 2x72 = 1 (3 pts)

Consider the equation mod 72 and we get:

29x5 ≡ 1 mod 72.

It follows that d = 29. (1 pt)

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

Solution
φ(n) = (p – 1)(q – 1) = (11 – 1)(17 – 1) = 160 (1 pt)

d = e^{-1} mod 160. Use the Extended Euclidean Algorithm to find 27^{-1} mod 160.

160 = 5x27 + 25
27 = 1x25 + 2
25 = 12x2 + 1 (2 pts)

25 – 12x2 = 1
25 – 12(27 – 25) = 1
25 – 12x27 + 12x25 = 1
13x25 – 12x27 = 1
13(160 – 5x27) – 12x27 = 1
13x160 – 65x27 – 12x27 = 1
13x160 – 77x27 = 1, taking this equation mod 160, we find
-77x27 ≡ 1 mod 160 (4 pts)

So, d ≡ -77 ≡ 83 mod 160, so d = 83. (1 pt)

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)?

Solution

$c_1 = g^k \bmod p = 11^4 \bmod 23 = (121)^2 \equiv 6^2 \equiv 13 \bmod 23$

$c_2 = Mb^k \bmod p = 6(14)^4 \bmod 23 = 6\,(196)^2 \equiv 6(12)^2 \equiv 6 \times 144 \equiv 6 \times 6 \equiv 13 \bmod 23.$

Grading: 3 pts for each

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?

Solution

Alice sends to Bob $8^6 \bmod 29 = (8^2)^3 \bmod 29 = 64^3 \equiv 6^3 \equiv 216 \equiv 13 \bmod 29$ (2 pts)

Bob sends to Alice $8^7 \bmod 29 = (8^6)(8) \bmod 29 \equiv 13(8) \equiv 104 \equiv 17 \bmod 29$ (2 pts)

The shared key computed by Alice is $17^6 \bmod 29$ and the shared key computed by Bob is $13^7 \bmod 29$. Here is the first computation:

$17^6 \equiv (-12)^6 \equiv ((-12)^2)^3 \equiv 144^3 \equiv (-1)^3 \equiv -1 \equiv 28 \bmod 29.$ (2 pts)

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 $g^a \bmod p$, user B calculates $g^b \bmod p$ and user C calculates $g^c \bmod p$. 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 $g^{ab} \bmod p$ to C, A sends $g^{ac} \bmod p$ 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 $g^{abc} \bmod p$. The key shared between A and B is $g^{ab} \bmod p$ the key shared between A and C is $g^{ac} \bmod p$ and the key shared between B and C is $g^{bc} \bmod p$.

What is the major flaw in this idea?

Solution

In the last step, C receives the secret key that is supposed to be shared by A and B only, B receives the secret key that is supposed to be shared by A and C only, and A receives the secret key that is supposed to be shared by B and C only. Thus, no secure communication can occur between any pair of individuals because the third individual has their shared key.

Grading: 4 pts, mostly all or nothing

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.

Solution

The public values are just each set value multiplied by 1645, then modded by 1836. Without the mod, the set is: {11515, 13160, 32900, 87185, 157920, 329000, 653065, 1345610}

Mod by 1836 to get the final public key set as: {499, 308, 1688, 893, 24, 356, 1285, 1658}

Grading: 4 pts, 1/2 pt for each item, round down

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

Solution

First let's find 2P:

$$\lambda = \frac{3(14^2)+2}{2(7)} \equiv 590(14^{-1}) \equiv 10(-2) \equiv -20 \equiv 9 mod 29$$
$$x = \lambda^2 - 2x_P = 9^2 - 2(14) = 81 - 28 = 53 \equiv 24 mod 29$$
$$y = \lambda(x_P - x) - y_P = 9(14 - 24) - 7 \equiv 30 - 14 \equiv 19 mod 29$$

Thus, 2P = (24, 19).

Grading: 3 pts for lambda(2 pts for mod inv), 1 pts for x, 1 pts for y

Now let's find P + Q:

$$\lambda = \frac{17-7}{26-14} \equiv 10(12^{-1}) \equiv 10(-12) \equiv -120 \equiv 25 mod 29$$
$$x = \lambda^2 - x_P - x_Q = 25^2 - 14 - 26 = 585 \equiv 5 mod 29$$
$$y = \lambda(x_P - x) - y_P = 25(14 - 5) - 7 \equiv 218 \equiv 15 mod 29$$

Thus, P + Q = (5, 15). Note that we can find 14^{-1} mod 29 and 12^{-1} mod 29 as follows:

29 = 2 x 14 + 1
29 - 2 x 14 = 1, so $14^{-1} \equiv -2$ mod 29

29 = 2 x 12 + 5	5 - 2 x 2 = 1
12 = 2 x 5 + 2	5 - 2(12 - 2 x 5) = 1
5 = 2 x 2 + 1	5 - 2 x 12 + 4 x 5 = 1
	5 x 5 - 2 x 12 = 1
	5 x (29 - 2x12) - 2 x 12 = 1
	5 x 29 - 12 x 12 = 1, so $12^{-1} \equiv -12$ mod 29

Grading: 3 pts for lambda(2 pts for mod inv), 1 pts for x, 1 pts for y

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

Solution

First let's find 2P:

$$\lambda = \frac{3(6^2) + 10}{2(14)} \equiv 118(28^{-1}) \equiv 2(-1) \equiv -2 \equiv 27 mod 29$$
$$x = \lambda^2 - 2x_P = 27^2 - 2(6) = 729 - 12 = 717 \equiv 21 mod 29$$
$$y = \lambda(x_P - x) - y_P = 27(6 - 21) - 14 \equiv 30 - 14 \equiv 16 mod 29$$

Thus, 2P = (21, 16).

Grading: 3 pts for lambda(2 pts for mod inv), 1 pts for x, 1 pts for y

Now let's find P + Q:

$$\lambda = \frac{20 - 14}{15 - 6} \equiv 6(9^{-1}) \equiv 6(13) \equiv 78 \equiv 20 mod 29$$
$$x = \lambda^2 - x_P - x_Q = 20^2 - 6 - 15 = 379 \equiv 2 mod 29$$
$$y = \lambda(x_P - x) - y_P = 20(6 - 2) - 14 \equiv 66 \equiv 8 mod 29$$

Thus, P + Q = (2, 8). Note that we can find 9's inverse mod 29 as follows:

29 = 3 x 9 + 2
9 = 4 x 2 + 1

9 - 4 x 2 = 1
9 - 4(29 - 3 x 9) = 1
9 - 4 x 29 + 12 x 9 = 1
13 x 9 - 4 x 29 = 1
Taking this equation mod 29, we find 13 x 9 ≡ 1 mod 29, so $9^{-1} \equiv 13 \pmod{29}$.

Grading: 3 pts for lambda(2 pts for mod inv), 1 pts for x, 1 pts for y