ECE371 Homework 2

PDF

ECE 371: Introduction to Security Engineering

Homework 2

1- Alice and Bob want to communicate with each other, and they agree to use Diffie-Hellman with prime $p = 17$ and generator $g = 3$.

(a) Alice picks $a = 4$ as her private key. What does she send to Bob?
(b) Bob picks $b = 11$ as his private key. What does he send to Alice?
(c) What is their shared secret key s? Show how Alice would compute it and how Bob would compute it.

2-Suppose you intercept a transmission between Alice and Bob, in which they agree to perform Diffie Hellman key exchange with $p = 23$ and $g = 15$. In the next message you intercept, you hear that Bob's public key is $B = 3$. What is Bob's private key?

3- Using RSA, choose $p = 13$ and $q = 17$, and encode the word "FLOOR" by encrypting each letter separately. Show the process of deriving n, d, e, and z. Each letter will be encrypted separately as a number between 1 and 26. Apply the decryption algorithm to the encrypted version to recover the original plaintext message. For both encryption and decryption provide a table as below to show the process:

Letter	m	m^e	ciphertext	c^d	c^d(mod N)	Decoded m
F	6					
L						
O						
O						
R						

1. Alice and Bob want to communicate with each other, and they agree to use Diffie-Hellman with prime p = 17 and generator g = 3.

a. Alice picks a = 4 as her private key. What does she send to Bob?

- $A = 3^4 \mod 17 = 13$ Alice sends A, 13 to Bob
  b. Bob picks b = 11 as his private key. What does he send to Alice?
- $B = 3^{11} \mod 17 = 7$ Bob sends B, 7 to Alice
  c. What is their s
- $s_a = B^a \mod p = 7^4 \mod 17 = 4$
- $s_b = A^b \mod p = 13^{11} \mod 17 = 4$

2. Suppose you intercept a transmission between Alice and Bob, in which they agree to perform Diffie-Hellman key exchange with p = 23 and g = 15. In the next message you intercept, you hear that Bob's public key is B = 3. What is Bob's private key?

- $B = 3$ is Bob's public key,
- $g = 15$ is the generator,
- $p = 23$ is the prime modulus.

We need to find an integer b such that:

$$15^b \equiv 3 \pmod{23}$$

doing this by simplifying is impossible so we need to

1. $15^1 \equiv 15 \pmod{23}$
2. $15^2 = 225 \equiv 18 \pmod{23}$
3. $15^3 = (15^2) * (15) = 18 * 15 = 270 \equiv 17 \pmod{23}$
4. $15^4 = (15^3) * (15) = 17 * 15 = 255 \equiv 2 \pmod{23}$
5. $15^5 = (15^4) * (15) = 2 * 15 = 30 \equiv 7 \pmod{23}$
6. $15^6 = (15)^5 * (15) = 7 * 15 = 105 \equiv 13 \pmod{23}$
7. $15^7 = (15)^6 * (15)^7 = 13 * 15 = 195 \equiv 11 \pmod{23}$
8. $15^8 = (15)^7 * (15) = 11 * 15 = 165 \equiv 4 \pmod{23}$
9. $15^9 = (15)^8 * (15) = 4 * 15 = 60 \equiv 14 \pmod{23}$

10. $15^{10} = (15)^9 * (15) = 14 * 15 = 210 \equiv 3 \pmod{23}$

Therefore, Bob's private key is:

$$b = 10$$

3. Using RSA, choose p = 13 and q = 17, and encode the word “FLOOR” by encrypting each letter separately. Show the process of deriving n, d, e, and z. Each letter will be encrypted separately as a number between 1 and 26. Apply the decryption algorithm to the encrypted version to recover the original plaintext message. For both encryption and decryption provide a table as below to show the process:

Letter	m	m^e	ciphertext $m^e \pmod{n}$	c^d	$c^d \pmod{n}$
F	6	279,936	150	4.8419382673e+119	6
L	12	35,831,808	194	6.74675820927e+125	12
O	15	170859375	76	2.78450226467e+103	15
O	15	170,859,375	76	2.78450226467e+103	15
R	18	612,220,032	86	2.49697858901e+106	18

$n = p * q = 13 * 17 = 221$

$\phi(n) = (p-1)(q-1) = 12 * 16 = 192$

e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$ easy choice is a positive prime smaller than $\phi(n)$, 7

$d =$ modular multiplicative inverse of $e \mod \phi(n)$

$d = 7 \pmod{192}$

to calculate this use the Extended Euclidean Algorithm

$gcd(7, 192) = 1$

$192 = 7 * 27 + 3$

$7 = 1 + 2 * 3$

$3 = 2 * 3$

sub in

$1 = 7 - 2 * 3$

$1 = 7 - 2(192 - 27 * 7)$

$1 = 7 - 2 * 192 + 54 * 7$
$1 = 55 * 7 - 2 * 192$
d = 55

n = 221, $\phi(n)$=192, e = 7, d = 55

4- Show that the following system of congruence has no solution: $x \equiv 4(mod 12)$ and $x \equiv 6(mod 18)$. You can start by writing the equation for congruence $(a \equiv b(modc) \rightarrow a - b = c * t)$ and then get to a contradictory result.

To show that the given system of congruences has no solution, we need to analyze the congruences:

1. $x \equiv 4 \pmod{12}$
2. $x \equiv 6 \pmod{18}$

$x = 12k + 4$
$x = 18m + 6$

since they are equivalent, they should equal each other

$12k + 4 = 18m + 6$
$12k - 18m = 2$
$2k - 3m = \frac{1}{3}$

since they subtract to a non integer, it shows that one of the variables must be a non whole number means there is no solution to the system of congruences, this is also because they are not co-prime numbers.