Intro to Security Homework 2

Taylor Foxhall

October 5, 2016

1 Problem 1

Alice's RSA public key is (N, e) = (33, 3), her private key is d = 7.

1.1 Part A

What is the ciphertext C if Bob encrypts M = 19 using Alice's public key?

$$C = M^e \mod N$$
$$M = C^d \mod N$$

So $C = 19^3 \mod 33 = 28$. Alice can decrypt this only if she knows N and d. Fortunately, N is known to everyone and d is known only to Alice. So $M = 28^7 \mod 33 = 19$, as we expect it to be.

1.2 Part B

If Alice signs S, what is S? And how can Bob verify that Alice signed S?

Alice can sign M by using her private key to encrypt M. So, $S = 25^7 \mod 33 = 31$, and then when she send M and S to Bob, he can try to decrypt S using her public key. Then he will check if D(S) and M match. We can compute $D(S) = 31^3 \mod 33 = 25 = M$. Since Alice is the only one who knows her private key, S must have been signed by Alice.

2 Problem 2

Alice wants to send Bob $g^a \mod p$ to Bob as in the Diffie-Hellman protocol. Bob wants the secret to be X. Can Bob choose his Diffie-Hellman value, $g^b \mod p$, such that the shared secret is X?

In order for this to be possible $X = g^{ab} \mod p$. So Bob must select b such that $X = (g^a)^b \mod p$. By doing a little modular arithmetic we can calculate b as

$$\begin{aligned} logX &= blog(g^a) \mod p \\ b &= logX * (log(g^a))^{-1} \mod p \end{aligned}$$

So provided Bob can solve $log(g^a)^{-1} \mod p$ he can choose b according to this restriction.

3 Problem 3

3.1 Part A

Given the curve $E : y^2 = x^3 + 7x + b$ find b so that $P = (4, 5)$ lies on it.

$$\begin{aligned} 5^2 &= 4^3 + 7(4) + b \mod 11 \\ 25 &= 92 + b \mod 11 \\ 3 &= 4 + b \mod 11 \\ b &= 10 \mod 11 \end{aligned}$$

3.2 Part B

List all points on E.

Since E is in the integers mod 11, we can check all integers x, $0 \leq x < 11$ for

solutions.

$$
\begin{aligned}
y^2 = (0)^3 + 7(0) + 10 = 10 \mod 11 &\quad \text{No solution.} \\
y^2 = (1)^3 + 7(1) + 10 = 7 \mod 11 &\quad \text{No solution.} \\
y^2 = (2)^3 + 7(2) + 10 = 10 \mod 11 &\quad \text{No solution.} \\
y^2 = (3)^3 + 7(3) + 10 = 3 \mod 11 &\quad y = 5, 6 \\
y^2 = (4)^3 + 7(4) + 10 = 3 \mod 11 &\quad y = 5, 6 \\
y^2 = (5)^3 + 7(5) + 10 = 5 \mod 11 &\quad y = 4, 7 \\
y^2 = (6)^3 + 7(6) + 10 = 4 \mod 11 &\quad y = 2, 9 \\
y^2 = (7)^3 + 7(7) + 10 = 6 \mod 11 &\quad \text{No solution.} \\
y^2 = (8)^3 + 7(8) + 10 = 6 \mod 11 &\quad \text{No solution.} \\
y^2 = (9)^3 + 7(9) + 10 = 10 \mod 11 &\quad \text{No solution.} \\
y^2 = (10)^3 + 7(10) + 10 = 2 \mod 11 &\quad \text{No solution.}
\end{aligned}
$$

So the points are $\{(3,5), (3,6), (4,5), (4,6), (5,4), (5,7), (6,2), (6,9), \mathbf{O}\}$.

3.3 Part C

Find the sum of $(4,5) + (5,4)$ on E.

$$
\begin{aligned}
c &= (4-5) * (5-4)^{-1} \mod 11 \\
&= -1 * (1)^{-1} \mod 11 \\
&= 10 * 1 \mod 11 \\
&= 10 \mod 11
\end{aligned}
$$

$$
\begin{aligned}
x_3 &= 10^2 - 4 - 5 \mod 11 \\
&= 91 \mod 11 \\
&= 3 \mod 11
\end{aligned}
$$

$$
\begin{aligned}
y_3 &= 10(4-3) - 5 \mod 11 \\
&= 5 \mod 11 \\
(4,5) + (5,4) &= (x_3, y_3) = (3,5)
\end{aligned}
$$

3.4 Part D

Find $3(4,5)$.

Since there's no direct way to compute $3(4,5)$ we must compute $(4,5)+(4,5)+(4,5)$ iteratively. We start with $(4,5)+(4,5)$.

$$\begin{aligned} c &= (3(4)^2+7)*(2(5))^{-1} \mod 11 \\ &= 0 \mod 11 \end{aligned}$$

$$\begin{aligned} (4,5)+(4,5) &= (0-4-4, 0(4-x_3)-5) \mod 11 \\ &= (3,6) \mod 11 \end{aligned}$$

And then we can calculate $(3,6)+(4,5)$.

$$\begin{aligned} c &= (5-6)*(4-3)^{-1} \mod 11 \\ &= 10 \mod 11 \end{aligned}$$

$$\begin{aligned} (3,6)+(4,5) &= (10^2-3-4, 10(3-x_3)-6) \\ &= (5, 10(9)-6) \\ &= (5,7) \end{aligned}$$

So $3(4,5) = (5,7)$.

4 Problem 4

Alice could find another key F, $F \neq K$, such that the output of decrypting Y with F would output an X different than what Bob told her if Bob's guess was correct. Bob has no way of knowing that she changed the keys, and so Alice could win everytime provided she could find a key that changes what X is. The way to fix that is for Alice to also send h(R) over along with Y, and when Bob decrypts Y with Alice's key he can verify that the hash Alice sent him matches the hash of the R he just decrypted using her key. It would be significantly more difficult for Alice to send him a different key that preserves h(R) but changes X in the decryption.