M/CS 478 Assignment 3

Isaac Boaz

March 7, 2024

2.17

(a) $11^x = 21$ in $\mathbb{F}_{71}$
Using Shanks's babystep-giantstep method, let's first populate the table for $[1, m]$ where $m = \lceil\sqrt{71}\rceil = 9$

11	50	53	15	23	40	14	12	61

Using Fermat's Little Theorem[1], we can find the 'bottom' cell of the table:

$$
\begin{aligned}
20x &\equiv 1 \pmod{71} \\
71 &= 3(20) + 11 \\
20 &= 1(11) + 9 \\
11 &= 1(9) + 2 \\
9 &= 4(2) + 1 \\
2 &= 2(1) + 0
\end{aligned}
$$

$$
\begin{aligned}
1 &= 9 - 4(2) \\
&= 9 - 4(11 - 9) \\
&= 5(9) - 4(11) \\
&= 5(20 - 11) - 4(11) \\
&= 5(20) - 9(11) \\
&= 5(20) - 9(71 - 3(20)) \\
&= 32(20) - 9(71) \\
20^{-1} &= 32 \pmod{71}
\end{aligned}
$$

Finally we multiply by the inverse to find the answer:

$$
\begin{aligned}
21 \times 32 &= 33 \pmod{71} \\
\times 32 &= 62 \pmod{71} \\
\times 32 &= 67 \pmod{71} \\
\times 32 &= 14 \pmod{71}
\end{aligned}
$$

Since 14 was in the top row, 7th column of the table, and we multiplied by the inverse (ie went up) 4 times, we know the correct cell is in the 7th column, 4th row. Thus $x = 3(10) + 7 = 37$. Plugging this back into the original equation, we get $11^{37} = 21 \pmod{71}$, which is true.

[1] Since 71 is a prime

3.7

Alice publishes her RSA public key: modulus $N = 2038667$ and exponent $e = 103$.

(a) Bob wants to send alice the message $m = 892383$. What ciphertext does Bob send to Alice? The formula for calculating ciphertext is

$$m^e \equiv c \pmod{N}$$

Thus, Bob simply needs to calculate

$$\begin{aligned} 892383^{103} &\equiv c \pmod{2038667} \\ c &\equiv 45293 \pmod{2038667} \end{aligned}$$

(b) Alice knows that her modulus factors into a product of two primes, one of which is $p = 1301$. Find a decryption exponent d for Alice.

We know that $N = 2038667 = p \cdot q$, and that e is the public exponent. We also know that d is the private exponent, and that d is the modular inverse of e mod $\phi(N)$. We can calculate $\phi(N)$ using the formula $\phi(N) = (p-1)(q-1)$.

$$\begin{aligned} \phi(N) &= (1301 - 1)(1567 - 1) \\ &= 1300 \cdot 1566 \\ &= 2035800 \end{aligned}$$

We can then calculate the modular inverse of e mod $\phi(N)$ using the extended Euclidean algorithm.

$$\begin{aligned} 2035800 &= 19765(103) + 5 \\ 103 &= 20(5) + 3 \\ 5 &= 1(3) + 2 \\ 3 &= 1(2) + 1 \end{aligned}$$

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (5 - 3) \\ &= 2(3) - 5 \\ &= 2(103 - 20(5)) - 5 \\ &= 2(103) - 41(5) \\ &= 2(103) - 41(2035800 - 19765(103)) \\ &= 810367(103) - 41(2035800) \\ 103^{-1} &= 810367 \pmod{2035800} \end{aligned}$$

Since $ed \equiv 1 \pmod{\phi(n)}$, $d = e^{-1} = 810367$.

(c) Alice receives the ciphertext $c = 317730$ from Bob. Decrypt the message. The formula for calculating the plaintext is

$$c^d \equiv m \pmod{N}$$

Thus, Alice simply needs to calculate

$$\begin{aligned} 317730^{810367} &\equiv m \pmod{2038667} \\ m &\equiv 514407 \pmod{2038667} \end{aligned}$$

Thus, Alice receives the message $m = 514407$.

3.11

Here is an example of a proposed public key system.

Alice chooses two large primces p and q and she publishes $N = pq$. It is assumed that N is hard to factor. Alice chooses three random numbers $g, r_1,$ and r_2 modulo N and computes

$$g_1 \equiv g^{r_1(p-1)} \pmod{N} \text{ and } g_2 \equiv g^{r_2(q-1)} \pmod{N}.$$

Her public key is the triple (N, g_1, g_2) and her private key is the pair of primes (p, q). Now Bob wants to send the message m to Alice where m is a number modulo N. He chooses two random integers s_1, s_2 modulo N and computes

$$c_1 \equiv m \cdot g_1^{s_1} \pmod{N} \text{ and } c_2 \equiv m \cdot g_2^{s_2} \pmod{N}.$$

Bob sends the ciphertext (c_1, c_2) to Alice. Alice decrypts the message using the Chinese Remainder Theorem.

$$x \equiv c_1 \pmod{p} \text{ and } x \equiv c_2 \pmod{q}$$

(a) Prove that Alice's solution x is equal to Bob's plaintext m.

$$\begin{aligned} c_1 &\equiv mg_1^{s_1} \pmod{p} \\ &\equiv mg^{r_1(p-1)^{s_1}} \pmod{p} \\ &\equiv mg^{r_1 s_1 (p-1)} \pmod{p} \\ &\equiv mg^{(p-1)^{r_1 s_1}} \pmod{p} \\ &\equiv m1^{r_1 s_1} \pmod{p} \\ &\equiv m \pmod{p} \\ c_2 &\equiv mg_2^{s_2} \\ &\equiv mg^{r_2(q-1)^{s_2}} \pmod{q} \\ &\equiv mg^{r_2 s_2 (q-1)} \pmod{q} \\ &\equiv mg^{(q-1)^{r_2 s_2}} \pmod{q} \\ &\equiv m \cdot 1^{r_2 s_2} \pmod{q} \\ &\equiv m \pmod{q} \end{aligned}$$

$$x \equiv c_1 \equiv m \pmod{p}$$
$$x \equiv c_2 \equiv m \pmod{q}$$

Since the CRT guarantees a unique solution modulo N, the solution that Alice finds *must* be equal to m.

$$x \equiv m \pmod{p}$$
$$x \equiv m \pmod{q}$$

(b) Since this uses the Chinese Remainder Theorem, m must be smaller than both p and q, otherwise CRT could return $m + xN$.

Additionally, given the two ciphertexts (c_1, c_2), the following attack is possible:

$$\begin{aligned} c_1 \cdot c_2^{-1} &\equiv (m \cdot g_1^{s_1})(m \cdot g_2^{s_2})^{-1} \\ &\equiv m^2 \cdot g_1^{s_1} \cdot g_2^{-s_2} \\ &\equiv m^2 \cdot (g^{r_1(p-1)^{s_1}}) \cdot (g^{r_2(q-1)^{-s_2}}) \\ &\equiv m^2 \cdot 1^{s_1} \cdot 1^{-s_2} \\ &\equiv m^2 \end{aligned}$$

3.13

Alice decides to use RSA with the public key $N = 1889570071$. In order to guard against transmission errors, Alice has Bob encrypt his message twice, once using the encryption exponent $e_1 = 1021763679$ and once using the encryption exponent $e_2 = 519424709$. Eve intercepts the two encrypted messages

$$c_1 = 1244183534 \text{ and } c_2 = 732959706$$

Assume Eve also knows N and the two ecnryption exponents e_1, e_2, help Eve recover Bob's plaintext without finding a factorization of N.

Since the $\gcd(c_1, c_2) = 1$, Eve can calculate a soultion to

$$e_1 \cdot u + e_2 \cdot v = 1$$

and then use u, v to calculate

$$\begin{aligned} c_1^u \cdot c_2^v &\equiv m^{e_1 \cdot u + e_2 \cdot v} \pmod{N} \\ &\equiv m^{\gcd(e_1, e_2)} \pmod{N} \\ &\equiv m^1 \end{aligned}$$

3.15

Use the Miller-Rabin test on each of the following numbers. In each case, either provide a Miller-Rabin witness for the compositeness of n, or conclude that n is probably prime by providing 10 numbers that are not Miller-Rabing withnesses for n.

(a) $n = 1105$

$$1105 - 1 = 2^4 \cdot 69 \qquad\qquad \text{thus } s = 4, d = 69$$

1. $a = 2$

$$\begin{aligned} x &= 2^{69} \pmod{1105} \\ &= 967 \\ x^2 &= 967^2 \pmod{1105} \\ &= 259 \\ x^4 &= 259^2 \pmod{1105} \\ &= 781 \\ x^8 &= 781^2 \pmod{1105} \\ &= 1,\ 1105 \text{ is composite} \end{aligned}$$

(b) $n = 294409$

$$294409 - 1 = 2^3 \cdot 36801 \qquad\qquad \text{thus } s = 3, d = 36801$$

1. $a = 2$

$$\begin{aligned} x &= 2^{36801} \pmod{294409} \\ &= 512 \\ x^2 &= 512^2 \pmod{294409} \\ &= 262144 \\ x^4 &= 262144^2 \pmod{294409} \\ &= 1,\ 294409 \text{ is composite} \end{aligned}$$

(e) $n = 118901521$

$$118901521 - 1 = 2^4 \cdot 7431345 \qquad\qquad \text{thus } s = 4, d = 7431345$$

1. $a = 2$

$$\begin{aligned} x &= 2^{7431345} \pmod{118901521} \\ &= 45274074 \\ x^2 &= 45274074^2 \pmod{118901521} \\ &= 1758249 \\ x^4 &= 1758249^2 \pmod{118901521} \\ &= 1,\ 118901521 \text{ is composite} \end{aligned}$$