MATH 135 Fall 2020: Extra Practice 9

Warm-Up Exercises

WE01. Given the public RSA encryption key $(e, n) = (5, 35)$, find the corresponding decryption key (d, n).

Solution. We factor n and find that $n = 5 \times 7$. Therefore, $p = 5$ and $q = 7$.

We can now find the decryption key d by solving $ed \equiv 1 \pmod{(p-1)(q-1)}$:

$$5d \equiv 1 \pmod{24}$$

By inspection, $d = 5$ is a solution. Because we have $1 < 5 < (p-1)(q-1)$, this is in fact the decryption key.

Therefore, the decryption key is $(5, 35)$. □

Recommended Problems

RP01. Suppose that in setting up RSA, Alice chooses $p = 47$, $q = 37$, and $e = 25$.

(a) What is Alice's public key?

Solution. We have $n = pq = 1739$, so Alice's pubkey is $(25, 1739)$. □

(b) What is Alice's private key?

Solution. We solve the congruence $ed \equiv 1 \pmod{(p-1)(q-1)}$ or $25d \equiv 1 \pmod{1656}$ which is equivalent to solving the LDE

$$25d + 1656y = 1$$

We do this with the good 'ole EEA:

y	d	r	q
1	0	1656	
0	1	25	
1	-66	6	66
-4	265	1	4

and conclude that $d = 265$ is a solution to our LDE. Since $1 < 265 < 1656$, it is in fact the decryption key. Therefore, Alice's privkey is $(265, 1739)$. □

(c) Suppose Alice wishes to send Bob the message $M = 20$. Bob's public key is $(23, 377)$ and Bob's private key is $(263, 377)$. What is the cipher text corresponding to M?

Solution. We compute the ciphertext C as $C \equiv M^e \pmod{n}$ where $0 \leq C < n$.

Substituting, $C \equiv 20^{23} \pmod{377}$. We perform the computation by hand like the masochistic math majors we are:

$$\begin{aligned} C &\equiv 20 \times 20^2 \times 20^4 \times 20^{16} \pmod{377} \\ &\equiv 20 \times 23 \times 23^2 \times 23^8 \pmod{377} \\ &\equiv 20 \times 23 \times 152 \times 152^4 \pmod{377} \\ &\equiv 20 \times 23 \times 152 \times 107^2 \pmod{377} \\ &\equiv 83 \times 152 \times 139 \pmod{377} \\ &\equiv 175 \times 139 \pmod{377} \\ &\equiv 197 \pmod{377} \end{aligned}$$

and since we have $0 \leq 197 < 377$, this is indeed our cyphertext. □

RP02. Set up an RSA scheme using two-digit prime numbers. Select values for the other variables and test encrypting and decrypting messages.

Solution. Let $p = 11$ and $q = 13$, the smallest two-digit prime numbers. Then, $n = pq = 143$. Choose e coprime to $(p-1)(q-1) = 120$ to be $e = 23$. To generate d, we solve $23d \equiv 1 \pmod{120}$, i.e., $23d + 120y = 1$, with the EEA:

y	d	r	q
1	0	120	
0	1	23	
1	−5	5	5
−4	21	3	4
5	−26	2	1
−9	47	1	1

Therefore, $d = 47$, and we have the pubkey $(23, 143)$ and privkey $(47, 143)$.

Suppose we want to send the ASCII exclamation mark "!", $M = 33$. Then, we compute the ciphertext $C \equiv M^e \pmod{n}$, i.e., $C \equiv 33^{23} \pmod{143}$. Expanding and reducing to the remainder, $C = 132$.

We decrypt by taking $R \equiv C^d \pmod{n}$, i.e., $R \equiv 132^{47} \pmod{143}$. Since in decryption we know p and q, we equivalently solve both

$$R \equiv 132^{47} \pmod{11} \quad \text{and} \quad R \equiv 132^{47} \pmod{13}$$

Simplifying by FℓT, we obtain

$$\begin{aligned} R &\equiv 132^7 \equiv 0 \pmod{11} \\ R &\equiv 132^{11} \equiv 7 \pmod{13} \end{aligned}$$

By the CRT, there is a unique solution modulo 143. We notice by inspection that $13(2) + 7 = 33 = 11(3)$, so $R = 33$ is the received message. □

Challenge

C01. Write a computer program to implement RSA encryption and decryption.

Solution. Allow me to demonstrate just how overpowered Wolfram Mathematica is:

```
(* Generates RSA keypair by default *)
keys = GenerateAsymmetricKeyPair[];
msg = "This is cheating";
cyphertext = Encrypt[keys["PublicKey"], msg];
received = Decrypt[keys["PrivateKey"], cyphertext];
```

Oh, you meant actually do the calculations? Okay.

```
(* Generate random primes below 100 *)
{p, q} = RandomPrime[100, 2]; n = p*q;
(* Generate e as a random coprime *)
m = (p-1)(q-1);
e = RandomChoice@Pick[Range[m], CoprimeQ[m, Range[m]]];
(* Solve d automagically *)
d = D /. Solve[e*D == 1, D, Modulus -> 120][[1]];

(* Sample encryption/decryption of 42 *)
C = PowerMod[42,e,n];
R = PowerMod[C,d,n];
```

□