Math 1350 RSA Example - August 3, 2010

Public Information

Corinne's key information: $m = 2573, e = 271$.

MGP's key information: $m = 3127, e = 69$.

We use A $\to$ 2, B $\to$ 3, ..., Z $\to$ 27.

Corinne sends `1915,2061,1222,1307` to MGP, and MGP sends `918, 2314,188` to Corinne.

Private Information

CORINNE'S PRIVATE INFORMATION

Corinne chooses $p = 31, q = 83$, and so $m = 2573$ and $n = (31-1)(83-1) = 30 \cdot 82 = 2460$. Since $e = 271$, we use the Euclidean Algorithm and to find d, the multiplicative inverse of 271 mod 2460. We find:

$$1 = 19 - 9(21-19) = 10(271 - 12\cdot 21) - 9\cdot 21 = 10\cdot 271 - 129(2460 - 9\cdot 271) = 1171\cdot 271 - 129\cdot 2460,$$

and so $d = 1171$.

Corinne wants to send the word `PLAY` to MGP, so the numerical equivalents are 17, 13, 2, 26. She calculates, using MGP's public m and e, $x^{e_{MGP}} \pmod{m_{MGP}}$, where x is each of 17, 13, 2, and 26. To do this, we calculate:

powers mod 3127	2	13	17
1	2	13	17
2	4	169	289
4	16	418	2219
8	256	2739	2063
16	2996	448	122
32	1526	576	2376
64	2188	314	1141

To get the 69th power, we multiply the 64th, 4th, and 1st powers, and we get:

$$17^{69} \equiv 1915 \pmod{3127}$$

$$13^{69} \equiv 2061 \pmod{3127}$$

$$2^{69} \equiv 1222 \pmod{3127}$$

$$26^{69} \equiv (2^{69} \cdot 13^{69}) \equiv 1307 \pmod{3127}$$

We then send the message: `1915, 2061, 1222, 1307` to MGP.
To decrypt `918,2314,188`, we calculate

powers mod 2573	918	2314	188
1	918	2314	188
2	1353	183	1895
4	1206	40	1690
8	691	1600	70
16	1476	2438	2327
32	1818	214	1337
64	1392	2055	1907
128	195	732	1000
256	2003	640	1676
512	702	493	1833
1024	1361	1187	2124

To get 1171, then we use that $1171 = 1024 + 128 + 16 + 2 + 1$, and so we multiply those powers together to get each number raised to the 1171.

$$918^{1171} \equiv 1361 \cdot 195 \cdot 1476 \cdot 1353 \cdot 918 \equiv 19 \pmod{2573}$$

$$2314^{1171} \equiv 1187 \cdot 732 \cdot 2438 \cdot 183 \cdot 2314 \equiv 20 \pmod{2573}$$

$$188^{1171} \equiv 2124 \cdot 1000 \cdot 2327 \cdot 1895 \cdot 188 \equiv 2 \pmod{2573}$$

We get our message from MGP as 19, 20, 2, which corresponds to `RSA`!

MGP'S PRIVATE INFORMATION

MGP choose their primes 53, 59, and so $m = 3127$ and $e = 69$. They find that $n = (53-1)\cdot(59-1) = 3016$, and so must find their d which is the multiplicative inverse of 69 modulo 3016.

MGP wants to send `RSA` to Corinne. The number equivalents are 17+2, 18+2, and 0+2, so 19, 20, and 2. They must raise each of these numbers to the 271 mod 2573, as this is Corinne's public modulus and encryption key. They calculate:

powers mod 2573	19	20	2
1	19	20	2
2	361	400	4
4	1671	474	16
8	536	825	256
16	1693	1353	1211
32	2500	1206	2484
64	183	691	202
128	40	1476	2209
256	1600	1818	1273

They need the 271st power, so they multiply the 256th power by the 8th,4th, 2nd, and 1st powers.

$$19^{271} \equiv 1600 \cdot 536 \cdot 1671 \cdot 361 \cdot 19 \equiv 918 \pmod{2573}$$

$$20^{271} \equiv 1818 \cdot 825 \cdot 474 \cdot 400 \cdot 20 \equiv 2314 \pmod{2573}$$

$$2^{271} \equiv 1273 \cdot 256 \cdot 16 \cdot 4 \cdot 2 \equiv 188 \pmod{2573}$$

The message they send is: `918, 2314, 188`.

MGP receives `1915, 2061, 1222, 1307` from Corinne, and to decrypt calculates:

powers mod 3127	1915	2061	1222	1307
1				
2				
4				
8				
16				
32				
64				
128				
256				
512				
1024				
2048				