Exercises: RSA

Note: For these exercises, you might want to use something like WolframAlpha for the computations: http://www.wolframalpha.com/
For example, to calculate $2^{10} \mod 15$ *type* "2ˆ10 mod 15".

1. Encrypt the word 'lion' using RSA with modulus $m = 1241$ and encryption key $E = 5$. The result will be four numbers between 0 and 1240.

   plaintext: l i o n

   in numbers: 11 8 14 13

   $p^E \mod m$: 962 502 471 234

   Note: The RSA computations are $11^5 \equiv 161051 \equiv 962 \mod 1241$, $8^5 \equiv 32768 \equiv 502 \mod 1241$, $14^5 \equiv 537824 \equiv 471 \mod 1241$, $13^5 \equiv 371293 \equiv 234 \mod 1241$.

2. (a) We want to create an RSA scheme with two primes $q_1 = 23$ and $q_2 = 179$. What is the modulus m?

   $m = 23 \times 179 = 4117$.

   (b) Using this scheme, calculate the value of A.

   $A = (23 - 1)(179 - 1) = 22 \times 178 = 3916$.

   (c) Using this scheme, what is the smallest possible choice of encryption key E?

   E must be coprime to A. Since $A = 3916 = 2^2 \times 11 \times 89$, then $E = 3$ will be coprime to A.

   (d) Use RSA and the smallest encryption key to encrypt the word 'badger'.

   plaintext: b a d g e r

   in numbers: 1 0 3 6 4 17

   $p^E \mod m$: 1 0 27 216 64 796

Note: Most of the RSA computations are simple, except $17^3 \equiv 4913 \equiv 796 \mod 4117$.

3. Decrypt the numbers '178, 163, 92, 161, 0, 106' using RSA with modulus $m = 187$ and decryption key $D = 3$. The resulting numbers should be turned back into letters of the alphabet.

ciphertext:	178	163	92	161	0	106
$p^D \mod m$:	19	14	20	2	0	13
plaintext:	t	o	u	c	a	n

Note: As an example, the first computation is $178^3 \equiv 5639752 \equiv 19 \mod 187$, although it is easier to calculate successive powers of $178 \mod 187$ and simplify each step as you go.

Questions 4 and 5 continue on the next pages.

4. (a) We want to create an RSA scheme with two primes $q_1 = 61$ and $q_2 = 223$. What is the modulus m?

   $m = 61 \times 223 = 13603$.

   (b) Using this scheme, calculate the value of A.

   $A = (61 - 1)(223 - 1) = 60 \times 222 = 13320$.

   (c) If the encryption key is $E = 1903$, what is the decryption key D?

   To find the decryption key, we need to find values D and t such that $1 = DE + tA$. This can be done by observation or using Euclid's algorithm:

$$\begin{aligned} 13320 &= (6)(1903) + 1902 \\ 1903 &= (1)(1902) + 1 \end{aligned}$$

   Reverse Euclid' Algorithm:

$$\begin{aligned} 1 &= (1)(1903) - (1)(1902) \\ &= (1)(1903) - (1)(13320 - (6)(1903)) = (7)(1903) - (1)(13320) \end{aligned}$$

   The decryption key is the coefficient of $E = 1903$, which is $D = 7$.

   (d) Use RSA and the decryption key to decrypt the numbers '12521, 12397, 10139, 99'.

ciphertext:	12521	12397	10139	99
$p^D \bmod m$:	15	14	13	24
plaintext:	p	o	n	y

5. (a) We want to create an RSA scheme with two primes $q_1 = 113$ and $q_2 = 257$. What is the modulus m?

$m = 113 \times 257 = 29041$.

(b) Using this scheme, calculate the value of A.

$A = (113 - 1)(257 - 1) = 112 \times 256 = 28672$.

(c) If the encryption key is $E = 18847$, what is the decryption key D?

To find the decryption key, we need to find values D and t such that $1 = DE + tA$. This can be done by using Euclid's algorithm.

$$\begin{aligned}
28672 &= 18847 + 9825 \\
18847 &= 9825 + 9022 \\
9825 &= 9022 + 803 \\
9022 &= (11)(803) + 189 \\
803 &= (4)(189) + 47 \\
189 &= (4)(47) + 1
\end{aligned}$$

Reverse Euclid' Algorithm:

$$\begin{aligned}
1 &= (1)(189) - (4)(47) \\
&= (1)(189) - (4)((1)(803) - (4)(189)) = (17)(189) - (4)(803) \\
&= (17)((1)(9022) - (11)(803)) - (4)(803) = (17)(9022) - (191)(803) \\
&= (17)(9022) - (191)((1)(9825) - (1)(9022)) = (208)(9022) - (191)(9825) \\
&= (208)((1)(18847) - (1)(9825)) - (191)(9825) = (208)(18847) - (399)(9825) \\
&= (208)(18847) - (399)((1)(28672) - (1)(18847)) = (607)(18847) - (399)(2867
\end{aligned}$$

The decryption key is the coefficient of $E = 18847$, which is $D = 607$.

(d) Use RSA and the decryption key to decrypt the numbers '27105, 6618, 0, 2549, 5757, 6496'.

ciphertext:	27105	6618	0	2549	5757	6496
p^D mod m:	15	4	0	13	20	19
plaintext:	p	e	a	n	u	t