

Encryption Example:

In order to understand how encryption works when implemented we will practice an example using small prime factors. Remember the security in encryption relies not on the algorithm but on the difficulty of deciphering the key. Here is an example using the RSA encryption algorithm.

Using RSA, choose $p = 5$ and $q = 7$, encode the phrase "hello". Apply the decryption algorithm to the encrypted version to recover the original plain text message.

Using the RSA encryption method we get the following steps:

- 1) Choose two prime numbers $p = 5$ and $q = 7$
- 2) Compute $n = pq$ and $z = (p - 1)(q - 1)$
 - a. $n = pq = (5)(7) = 35$
 - b. $z = (p - 1)(q - 1) = (5 - 1)(7 - 1) = (4)(6) = 24$
- 3) Choose a number $e < n$ such that it has no common factors with z other than 1
 - a. Let $e = 5$
- 4) Find a number d such that ed divided z has a remainder of 1
 - a. Using the extended Euclidean algorithm to find the inverse modulo 35 find $d = 29$
- 5) The public key becomes K^+_B or the number pair (n, e) and the private key becomes K^-_B or the number pair (n, d)

Thus, the encrypted value c of the plain text message m is:

$$c = m^e \bmod n$$

Now, using the alphabet such that the letters are numbered 1 through 26 we get

Plain Text	h	e	l	l	o
Number	8	5	12	12	15
Encrypted value	8	10	17	17	15

Where,

$$8^5 \bmod 35 = 8$$

$$5^5 \bmod 35 = 10$$

$$12^5 \bmod 35 = 17$$

$$12^5 \bmod 35 = 17$$

$$15^5 \bmod 35 = 15$$

This gives the encrypted value of the word "hello" as 8 10 17 17 15 where:

$h \rightarrow 8, e \rightarrow 10, l \rightarrow 17, l \rightarrow 17, o \rightarrow 15$

In order to decrypt the message c , calculate:

$$m = c^d \bmod n$$

Thus, we get:

Encrypted value	8	10	17	17	15
Number	8	5	12	12	15
Plain Text	h	e	l	l	o

This gives the encrypted value of 8 10 17 17 15 as the word "hello" where:

$8 \rightarrow h, 10 \rightarrow e, 17 \rightarrow l, 17 \rightarrow l, 15 \rightarrow o$

Which is the word "hello". Of course if the message was encrypted using the ASCII values of the letters for the plain text, the lower and upper case letters could be differentiated.