RSA DECRYPTION EXAMPLE

Using ENCRYPTION Keys: $N = pq = 713$
where $p = 23$ and $q = 31$.

$$(\text{So, } (p-1)(q-1) = 22 \times 30 = 660)$$

The other Key e = any positive integer that is relatively prime to $(p-1)(q-1)$.

For instance, we can use $e = 43$ since $\gcd(43, 660) = 1$.
43 is prime and $660 = 20 \times 30$.

Task: Decrypt the received ciphertext $C = 129$.

Decryption Rule: Plaintext $M = C^d \bmod pq$
where
d is an inverse of $e \pmod{(p-1)(q-1)}$.

Here, we can use $d = 307$ since 307 is a (mod 660) inverse of $e = 43$.

That is, $(43)(307) \equiv 1 \pmod{660}$

Sol'n: $M = (129)^{307} \bmod 713$

$307 = 256 + 32 + 16 + 2 + 1$

$$(129)^{307} = (129)^{256} \cdot (129)^{32} \cdot (129)^{16} \cdot (129)^{2} \cdot (129)^{1}$$

See the report from the Power Calculator.

$$(129)^{307} \equiv (315) \cdot (87) \cdot (284)(242)(129) \pmod{713}$$

$$(315) \cdot (87) \equiv 311 \pmod{713}$$

$$(284) \cdot (242) \equiv 280 \pmod{713}$$

$$(280) \cdot (129) \equiv 470 \pmod{713}$$

$$(311) \cdot (470) \equiv 5 \pmod{713}$$

$\therefore (129)^{307} \equiv 5 \pmod{713}$ and $0 \le 5 < 713$.

$\therefore$ By Thm(W13)6, $\left((129)^{307} \bmod 713\right) = 5$.

The message sent and received is "E".

Power Calculator (mod n) and Modular Multipler

Given values for "a" and "n",
calculate (a^(2^k) mod n)
for k = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9

Enter *a* here ---> a = 129 modulus n = 713 <--- Enter *n* here.

k	Calculation	X	times	Y	≡	Z	(mod	n	)
0	1xa	1		129	≡	129	(mod	713	)
1	a x a	129	×	129	≡	242	(mod	713	)
2	a^2 x a^2	242	×	242	≡	98	(mod	713	)
3	a^4 x a^4	98	×	98	≡	335	(mod	713	)
4	a^8 x a^8	335	×	335	≡	284	(mod	713	)
5	a^16 x a^16	284	×	284	≡	87	(mod	713	)
6	a^32 x a^32	87	×	87	≡	439	(mod	713	)
7	a^64 x a^64	439	×	439	≡	211	(mod	713	)
8	a^128 x a^128	211	×	211	≡	315	(mod	713	)
9	a^256 x a^256	315	×	315	≡	118	(mod	713	)

Summary of Powers (mod n)

a = 129

(a^(2^k)	mod	713	) =	Z
(a	mod	713	) =	129
(a^2	mod	713	) =	242
(a^4	mod	713	) =	98
(a^8	mod	713	) =	335
(a^16	mod	713	) =	284
(a^32	mod	713	) =	87
(a^64	mod	713	) =	439
(a^128	mod	713	) =	211
(a^256	mod	713	) =	315
(a^512	mod	713	) =	118

Modular Multiplier

Modulus n = 713 The modulus value n is the same as above.

X	x	Y	≡	Z	(mod	n	)
315	x	87	≡	311	(mod	713	)
284	x	242	≡	280	(mod	713	)
280	x	129	≡	470	(mod	713	)
311	x	470	≡	5	(mod	713	)
1	x	1	≡	1	(mod	713	)
1	x	1	≡	1	(mod	713	)