Example:

* The plaintext consists of all 256 7-bit ASCII character codes in hexadecimal.
* Given a plaintext **M = 506574**, determine the encryption of M, using C = Mg mod n.
* C also refers to the ciphertext of the plaintext M.
* Select a public key, e = g = 59,
* Select two private keys p = 991 and q = 997.
* Compute a public key, n = pq = 988027
* Those who have the public keys, g = 59 and n, should be able to compute the ciphertext of the plaintext M.
* Only the person who knows two private keys, p and q, can compute (n) = (p – 1) (q – 1) = 990 \* 996 = **986040.**
* Encode: C = Me (mod pq), where e (also called g) = 59, and
* 59 = 32 + 16 + 8 + 2 + 1
* i.e., the bit representation for 59 is 111011.
* To encode M, compute C = Me (mod pq)
* = 50657459 (% 988027)
* = 506574(32+16+8+2+1) (% 988027) = 661578

Here is the computation:

Give **M = 506574** and n = pq = 988027.

M mod n = *506574*

M\*\*2 mod n ≡ 5065742 mod 988027 = *916874*

M\*\*4 mod n ≡ 9168742 mod 988027 = 99061

M\*\*8 mod n ≡ 990612 mod 988027 = *985584*

M\*\*16 mod n ≡ 9855842 mod 988027 = *40087*

M\*\*32 mod n ≡ 400872 mod 988027 = *435667*

50657459 (mod 988027)

≡ (50657432 \* 50657416 \* 5065748 \* 5065742 \* 506574)(mod 988027)

≡ ((506574)(mod 988027) \* (5065742)(mod 988027) \* (5065748)(mod 988027) \* (50657416)(mod 988027)\* (50657432)(mod 988027)) mod 988027

≡ (506574 \* 916874 \* 985584 \* 40087 \* 435667) mod 988027

≡ (((((((506574 \* 916874)mod 988027) \* 985584) mod 988027) \*

40087) mod 988027) \* 435667) mod 988027

x≡ (((((941192 \* 985584) mod 988027) \* 40087) mod 988027) \* 435667) mod 988027

≡ (((794800 \* 40087) mod 988027) \* 435667) mod 988027

≡ (240931 \* 435667)mod 988027

= 661578

***The ciphertext of the plaintext 506574 is*** **661578**

***That is, C = 661578***

***Everyone in the community knows C = 661578 with e = 59 and n =* 988027**.