* For getting the decryption of C, apply M = Ch mod n. How do you get the plaintext M of the ciphertext C?
* You need to have the secret keys, p, q, and h, where h = g-1 mod $φ$(n).
* h is called the multiplicative inverse of g mod $φ\left(n\right).$ In other words, compute the multiplicative inverse, $[h]\_{φ\left(n\right) } of  [g]\_{φ(n)}. $
* **Strategy**: Compute a GCD as a Linear Combination. Then, find an inverse Modulo n. In other words, you can apply the extended Euclid algorithm to find the linear combination of g and $φ\left(n\right).$ Then, find a positive inverse of g mod $φ\left(n\right).$
* Find a positive inverse of 59 (mod $φ$(n) ) = 59 (mod 986040), where $φ$(n) = (p – 1) (q – 1) = 990 \* 996 = **986040.**

To find a positive inverse of 59 (mod (p-1)(q-1)) = 59 (mod 986040), we need to

compute first a GCD ($φ$(n), g) as a Linear Combination, which is as follows:

gcd(986040, 59) 986040 = 16712 \* 59 + 32 implies 32 = 1\*986040 - 16712 \* 59

 Bottom-Up calculation: 1 = -13\*59 + 24\*(986040 - 16712\*59)

 1 = 24\*986040 – 401101\*59

 We obtain the linear combination for the GCD.

= gcd(59, 32) 59 = 1 \* 32 + 27 implies 27 = 1\*59 – 1\*32

Bottom-Up calculation: 1 = 11\*32 – 13\*(59 - 1\*32)

 1 = -13\*59 + 24\*32

= gcd(32, 27) 32 = 1 \* 27 + 5 implies 5 = 1\*32 – 1\*27

Bottom-Up calculation: 1 = -2\*27 + 11\*5

 1 = -2\*27 + 11\*(1\*32 - 1\*27)

 1 = 11\*32 – 13\*27

= gcd(27, 5) 27 = 5 \* 5 + 2 implies 2 = 1 \* 27 – 5 \* 5

 Bottom-Up calculation: 1 = 1\*5 – 2\*2

 1 = 1\*5 – 2\*(1\*27 - 5\*5)

 1 = -2\*27 + 11\*5

= gcd(5, 2) 5 = 2 \* 2 + 1 implies 1 = 1 \* 5 – 2 \*2

Bottom-Up calculation: 1 = 1\* 1 = 1\*(5 - 2 \* 2)

 1 = 1\*5 – 2\*2

= gcd(2, 1) 2 = 2 \* 1 + 0 implies 0 = 1 \* 2 – 2 \* 1

Bottom-Up calculation: 1 = 1 \* 1 - 0 \* 0

1 = 1 \* 1 - 0 \*(1\*2 - 2\*1)

 1 = 1 \* 1

= gcd(1, 0) 1 = 0 \* 0 + 1 implies 1 = 1 \* 1 - 0 \* 0

1 = 1 \* 1 - 0 \* 0

= 1

We have the linear combination for GCD($φ$(n), g) = GCD(986040, 59)

1 = 24\*986040 - 401101\*59

1 (mod 986040)$≡($24\*986040 – 401101\*59)(mod 986040)

1 (mod 986040)$≡ $(24\*986040(mod 986040)

 – 401101\*59(mod 986040))(mod 986040)

1 (mod 986040)$≡ $(0 – 401101\*59)(mod 986040)

1 (mod 986040)$≡$ -401101\*59 (mod 986040)

1(mod 986040) $≡$ -401101\*59 (mod 986040)

-401101\*59 (mod 986040)$ ≡$ 1(mod 986040)

-401101$ ≡$ $\frac{1}{59}$(mod 986040)

-401101 is the multiplicative inverse of 59.

We need to get the smallest positive multiplicative inverse of 59:

-401101 + 986040 = 584939 is the smallest positive multiplicative inverse of 59

The secret key is ( 988027, **584939**)

The secret key is (p=991, q=997, h=**584939)**

No one in this community can get this h without the value of p and q.

Decode:

What is the decryption of C using M = Ch mod n? How to obtain M, which is the plaintext M of the ciphertext C.

The secret key is (p=991, q=997, h=**584939).**

n = p \* q = 991 \* 997 = 988027

d = h = **584939**

**C = 661578 --- the ciphertext of M**

Decode: M = Cd (Mod pq)

 M = **661578**584939 mod 988027

The above equation also requires a large computation time.

Computation Steps will be as follows:

584939 =219 + 215 + 214 + 213 + 211 +210 +27 + 26 + 25 +23 + 2 + 1

 = 1 + 2 + 8 + 32 + 64 + 128 + 1024 + 2048 + 8192 +

16384 + 32768 + 524288

Enter C **661578**, d 584939, pq 988027

**661578 mod 988027 = 661578**

**661578**2 mod 988027 = **357381**

**661578**4 mod 988027 = **904925**

**661578**8 mod 988027 = **621701**

**661578**16 mod 988027 = **911136**

**661578**32 mod 988027 = **860340**

**661578**64 mod 988027 = **536442**

**661578**128 mod 988027 = **239425**

**661578**256 mod 988027 = **980139**

**661578**512 mod 988027 = **962870**

**661578**1024 mod 988027 = **537369**

**661578**2048 mod 988027 = **719033**

**661578**4096 mod 988027 = **602718**

**661578**8192 mod 988027 = **112407**

**661578**16384 mod 988027 = **444373**

**661578**32768 mod 988027 = **286909**

**661578**65536 mod 988027 = **292803**

**661578**131072 mod 988027 = **517965**

**661578**262144 mod 988027 = **865699**

**661578**524288 mod 988027 = **470669**

Decode: M = Cd (Mod pq)

M = **433940**584939 mod 988027

M = (**661578** \* **357381** \* **621701** \* **860340** \* **536442** \* **239425** \* **537369** \* **719033** \* **112407** \* **444373** \* **286909** \* **470669**) mod 988027

M = (((((((((((((((((((((((**661578** \* 357381)mod 988027) \* **621701**)mod 988027) \* **860340**)mod 988027) \* **536442**)mod 988027) \* **239425**)mod 988027) \* **537369**)mod 988027) \* **719033**)mod 988027) \* **112407**)mod 988027) \* **444373**)mod 988027) \* **286909**)mod 988027) \* **470669**)mod 988027)mod 988027

= 506574 (You may get 132840 as the solution, but it is wrong!)

The calculation process is as follows:

Since n = 988027

(**661578** \* 357381)mod 988027= 546118

(546118 \* 621701) mod n = 460546

(460546 \* **860340**) mod n = 641911

M = (((((((((((((((((((((((**661578** \* 357381)mod 988027) \* **621701**)mod 988027) \* **860340**)mod 988027) \* **536442**)mod 988027) \* **239425**)mod 988027) \* **537369**)mod 988027) \* **719033**)mod 988027) \* **112407**)mod 988027) \* **444373**)mod 988027) \* **286909**)mod 988027) \* **470669**)mod 988027)mod 988027

(mod1\_2\_8\_32 \* mod64)mod n

= (641911 \* **536442**)mod 988027 = 850622

(mod1\_2\_8\_32\_64 \* mod128)mod n

= (850622 \* **239425**)mod 988027 = 142894

(mod1\_32\_64\_128 \* mod1024)mod n

= (142894 \* **537369**)mod 988027 =311527

(mod1\_32\_64\_128\_1024 \* mod2048) mod n

= (311527 \* **444373**) mod 988027 = **616167**

(mod1\_32\_64\_128\_2048 \* mod8192)mod n

= (616167 \* **112407**) mod 988027 = **791269**

(mod1\_128\_2048\_8192 \* mod16384)mod n

= (791269 \* **444373**) mod 988027 = 518604

(mod1\_2048\_8192\_16384 \* mod32768)mod n

= (518604 \* **286909**) mod 988027 = **228971**

(mod1\_8192\_16384\_32768 \* mod424288)mod n

= (228971 \* **470669**) mod 988027 = **506574**

Therefore, M is 506574

The plaintext M for the ciphertext 661578 is:

The decryption of C using M = Ch mod n

M = **661578**584939 mod 988027

 = **506574**