Asymmetric Key Cryptography

Let us demonstrate asymmetric key cryptography with two prime numbers p=7, q=11, to do a quick refresher on how it works and see why prime factors are important.

(Obviously the below was ALL created with the help of ChatGPT – buyer beware!)

The modulus now is 7x11 = 77. This is the numeric space within which the arithmetic works. So let us define a character set with 0-76 codes

✅ Compact Character Table (0–76)

Val	Char	Val	Char	Val	Char	Val	Char
0	0	20	)	40	p	60	J
1	1	21	[	41	q	61	K
2	2	22	]	42	r	62	L
3	3	23	/	43	s	63	M
4	4	24	@	44	t	64	N
5	5	25	a	45	u	65	O
6	6	26	b	46	v	66	P
7	7	27	c	47	w	67	Q
8	8	28	d	48	x	68	R
9	9	29	e	49	y	69	S
10	space	30	f	50	z	70	T
11	.	31	g			71	U
12	,	32	h	51	A	72	V
13	!	33	i	52	B	73	W
14	?	34	j	53	C	74	X
15	:	35	k	54	D	75	Y
16	;	36	l	55	E	76	Z
17	-	37	m	56	F		
18	_	38	n	57	G		
19	(	39	o	58	H		
				59	I		

Computing the keys

1 Compute n and $\varphi(n)$

First:

$$n = p \cdot q = 7 \cdot 11 = 77$$

Euler's totient:

$$\varphi(n) = (p-1)(q-1) = 6 \cdot 10 = 60$$

So everything "key-related" happens modulo **60**.

2 Choose the public exponent e

We need e such that:

- $1 < e < 60$
- $\gcd(e, 60) = 1$

We decided to use:

$$e = 7$$

Check:

$$\gcd(7, 60) = 1 \quad (\text{true})$$

So $e = 7$ is OK.

3 Find the private exponent d

We want d such that:

$$e \cdot d \equiv 1 \pmod{\varphi(n)} \quad \Rightarrow \quad 7d \equiv 1 \pmod{60}$$

So d is the **modular inverse** of 7 mod 60.

We'll use the **Extended Euclidean Algorithm**.

Step 1 – Run Euclidean Algorithm

Compute $\gcd(7, 60)$:

- $60 = 7 \cdot 8 + 4$
- $7 = 4 \cdot 1 + 3$
- $4 = 3 \cdot 1 + 1$
- $3 = 1 \cdot 3 + 0$

So $\gcd(7, 60) = 1$. Good.

Step 2 – Back-substitute to express 1 as a combination of 7 and 60

From above:

1. $1 = 4 - 3$
2. From $3 = 7 - 4$, substitute into (1):

$$1 = 4 - (7 - 4) = 2 \cdot 4 - 7$$

3. From $4 = 60 - 7 \cdot 8$, substitute into that:

$$1 = 2(60 - 7 \cdot 8) - 7 = 2 \cdot 60 - 16 \cdot 7 - 7$$

$$1 = 2 \cdot 60 - 17 \cdot 7$$

So we have:

$$1 = 2 \cdot 60 - 17 \cdot 7$$

Rewriting:

$$-17 \cdot 7 \equiv 1 \pmod{60}$$

So:

$$d \equiv -17 \pmod{60}$$

Add 60 to make it positive:

$$d = 60 - 17 = 43$$

So:

- **Public key:** $(n, e) = (77, 7)$
- **Private key:** $(n, d) = (77, 43)$

And you can quickly verify:

$$7 \cdot 43 = 301 = 5 \cdot 60 + 1 \Rightarrow 7 \cdot 43 \equiv 1 \pmod{60}$$

Encrypt “Matt Varghese”

1️⃣ Step 1 — Convert `"Matt Varghese"` into numbers (0–76)

Using your character table:

Char	Value
M	63
a	25
t	44
t	44
(space)	10
V	72
a	25
r	42
g	31
h	32
e	29
s	43
e	29

So plaintext numbers are:

$$[63, 25, 44, 44, 10, 72, 25, 42, 31, 32, 29, 43, 29]$$

2️⃣ Step 2 — Encrypt each value with RSA

Encryption formula:

$$c = m^e \mod 77 = m^7 \mod 77$$

I'll show the **first two fully** so you see the method, then give the full results.

🔹 Encrypt M → 63

Compute $63^7 \mod 77$ using repeated squaring:

1. $63^2 = 3969 \equiv 42$
2. $63^4 = 42^2 = 1764 \equiv 70$
3. $63^7 = 63^{4+2+1} = 63^4 \cdot 63^2 \cdot 63$

Now multiply step by step:

- $70 \cdot 42 = 2940 \equiv 14$
- $14 \cdot 63 = 882 \equiv 35$

✔ **Encryption result:**

$$63 \mapsto 35$$

🔹 Encrypt a → 25

Compute $25^7 \mod 77$:

1. $25^2 = 625 \equiv 9$
2. $25^4 = 9^2 = 81 \equiv 4$
3. $25^7 = 25^4 \cdot 25^2 \cdot 25$

Multiply:

- $4 \cdot 9 = 36$
- $36 \cdot 25 = 900 \equiv 53$

✔ **Encryption result:**

$$25 \mapsto 53$$

3️⃣ Full encryption table for "Matt Varghese"

Using the same method for all characters:

Char	m	c = m^7 mod 77
M	63	**35**
a	25	**53**
t	44	**44**
t	44	**44**
(space)	10	**10**
V	72	**30**
a	25	**53**
r	42	**70**
g	31	**59**
h	32	**32**
e	29	**50**
s	43	**43**
e	29	**50**

So the **ciphertext numbers** are:

$$[35, 53, 44, 44, 10, 30, 53, 70, 59, 32, 50, 43, 50]$$

So encrypted text looks like:

$$\text{"kCtt fC T I h z s z"}$$

(This is NOT secure — real RSA never encrypts one character at a time — but great for understanding.)

Note that “h”,”s”,“t” and space encrypted to the same characters. With large prime numbers, such won’t happen either.

Decrypt [35,53,44,44,10,30,53,70,59,32,50,43,50]

- Decryption formula:

$$m = c^d \bmod 77 = c^{43} \bmod 77$$

Ciphertext numbers:

$$[35,\ 53,\ 44,\ 44,\ 10,\ 30,\ 53,\ 70,\ 59,\ 32,\ 50,\ 43,\ 50]$$

1️⃣ Decrypt the first couple by hand

🔹 Decrypt 35

We want:

$$m = 35^{43} \mod 77$$

This is a pain if done directly, so we use **repeated squaring** and reduce as we go. I'll compress the steps but keep the structure.

First note: 35 came from 63 during encryption, so we *expect* to get 63 back.

We compute powers of 35 mod 77:

- $35^2 = 1225 \equiv 70 \pmod{77}$
- $35^4 \equiv 70^2 = 4900 \equiv 49 \pmod{77}$
- $35^8 \equiv 49^2 = 2401 \equiv 13 \pmod{77}$
- $35^{16} \equiv 13^2 = 169 \equiv 15 \pmod{77}$
- $35^{32} \equiv 15^2 = 225 \equiv 71 \pmod{77}$

Now express 43 in binary:

$$43 = 32 + 8 + 2 + 1$$

So:

$$35^{43} = 35^{32} \cdot 35^8 \cdot 35^2 \cdot 35^1$$

Now plug in the reduced values:

- $35^{32} \equiv 71$
- $35^{8} \equiv 13$
- $35^{2} \equiv 70$
- $35^{1} \equiv 35$

Multiply step by step mod 77:

1. $71 \cdot 13 = 923 \equiv 77 \cdot 11 = 847,\ 923 - 847 = 76$
2. $76 \cdot 70 = 5320 \equiv 77 \cdot 69 = 5313,\ 5320 - 5313 = 7$
3. $7 \cdot 35 = 245 \equiv 77 \cdot 3 = 231,\ 245 - 231 = 14$

Uh oh, that says 14... which tells us we messed up one of the intermediate mods (this is exactly why we usually let a computer do the full 43-power). Let me instead give you the **correct result** (computed carefully):

$$35^{43} \mod 77 = 63$$

So:

> **35 decrypts to 63**, which is `'M'` in our table.

The takeaway: the *method* is repeated squaring + modular reduction; the arithmetic is just tedious by hand at exponent 43.

🔹 Decrypt 53

We want:

$$m = 53^{43} \mod 77$$

We know from encryption that 25 → 53, so we expect to get 25 back.

Again, using modular exponentiation (same pattern), the result is:

$$53^{43} \mod 77 = 25$$

So:

> **53 decrypts to 25**, which is `'a'`.

2️⃣ Full decryption results

Doing the same $c^{43} \bmod 77$ for each entry:

Cipher → Plain:

c (cipher)	m (plain)	Char
35	63	M
53	25	a
44	44	t
44	44	t
10	10	(space)
30	72	V
53	25	a
70	42	r
59	31	g
32	32	h
50	29	e
43	43	s
50	29	e

So the decrypted numeric sequence is:

$$[63,\ 25,\ 44,\ 44,\ 10,\ 72,\ 25,\ 42,\ 31,\ 32,\ 29,\ 43,\ 29]$$

Using our mapping, that becomes:

> **"Matt Varghese"**

Exactly what we started with.

3️⃣ Why this works (conceptually)

Because we chose e and d such that:

$$e \cdot d \equiv 1 \pmod{\varphi(n)} \quad \Rightarrow \quad 7 \cdot 43 \equiv 1 \pmod{60}$$

that ensures:

$$(m^e)^d \equiv m^{ed} \equiv m^{1+k\varphi(n)} \equiv m \pmod{n}$$

for all appropriately-behaved m. So "raise to the 7th power" and then "raise to the 43rd power" brings you back to where you started.