RSA example

1) $p = 43,\ q = 59$
2) $n = p \cdot q = 2537$
3) $e = 13$

   $(p-1)(q-1) = 42 \cdot 58 = 2436$

   $\gcd(13, 2436) = 1$
4) $\gcd(2436, 13)$

   $= \gcd(13, 5)$

   $= \gcd(5, 3)$

   $= \gcd(3, 2)$

$2436 = 187 \cdot 13 + 5$ $\overset{(4)}{\Rightarrow}$ $5 = 2436 - 187 \cdot 13$

$13 = 2 \cdot 5 + 3$ $\overset{(3)}{\Rightarrow}$ $3 = 13 - 2 \cdot 5$

$5 = 1 \cdot 3 + 2$ $\overset{(2)}{\Rightarrow}$ $2 = 5 - 1 \cdot 3$

$3 = 2 \cdot 1 + 1$ $\overset{(1)}{\Rightarrow}$ $1 = 3 - 2 \cdot 1$

$\Rightarrow 1 \overset{(1)}{=} 3 - 2 \cdot 1 \overset{(2)}{=} 3 - 2 \cdot (5 - 1 \cdot 3) = 2 \cdot 3 - 5 \overset{(3)}{=} 2 \cdot (13 - 2 \cdot 5) - 5 = 2 \cdot 13 - 5 \cdot 5$

$\overset{(4)}{=} 2 \cdot 13 - 5 \cdot (2436 - 187 \cdot 13) = 937 \cdot 13 - 5 \cdot 2436$

$\Rightarrow 937 \cdot 13 \equiv 1 \pmod{2436}$

$\Rightarrow d = 937$

5) $P_A = (13, 2537)$
6) $S_A = (937, 2537)$

Encryption example: Encrypt the message STOP using RSA for Alice

1) Translate letters to numbers

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

2) Translate message to numbers:

S T O P

18 19 14 15

3) Use our RSA example: $n = 2537 = 43 \cdot 59$

$e = 13$

$d = 937$

$\mathbb{Z}_n = \{0, 1, \ldots, 2536\}$

Group digits into blocks of four in order to have message $m_i \in \mathbb{Z}_n$:

$\underbrace{1819}_{m_1} \; \underbrace{1415}_{m_2}$

4) Encrypt m_i:

$m_1 \downarrow \quad m_2 \downarrow$

$c_1 \quad c_2$

2081 2182

$c_1 = 1819^{13} \pmod{2537} = 2081$

$c_2 = 1415^{13} \pmod{2537} = 2182$

Check that decrypting the encrypted message will yield the original message:

$2081^{937} \pmod{2537} = 1819$ ✓

$2182^{937} \pmod{2537} = 1415$ ✓