Encrypt the plaintext 'security' using the RSA algorithm for the values $p_B = 7$, $q_B = 11$ and $e_B = 13$.

Solution

Encryption:

Plaintext = security

plaintext (p) :

Plaintext	**s**	**e**	**c**	**u**	**r**	**i**	**t**	**y**
Numeric notation	18	4	2	20	17	8	19	24

Ciphertext	Encryption	Encryption result
Ciphertext (C_1)	$18^{13} \bmod 77$	46
Ciphertext (C_2)	$4^{13} \bmod 77$	77
Ciphertext (C_3)	$2^{13} \bmod 77$	30
Ciphertext (C_4)	$20^{13} \bmod 77$	69
Ciphertext (C_5)	$17^{13} \bmod 77$	7
Ciphertext (C_6)	$8^{13} \bmod 77$	50
Ciphertext (C_7)	$19^{13} \bmod 77$	61
Ciphertext (C_8)	$24^{13} \bmod 77$	52
Ciphertext (C): 46 77 30 69 7 50 61 52		

Decryption:

Ciphertext (C): **46 77 30 69 7 50 61 52**

Key generation in Bob side:

1. $n_B = p_B \times q_B = 7 \times 11 = 77$
2. $\varphi(n_B) = (p_B - 1) \times (q_B - 1) = (7 - 1) \times (11 - 1) = 6 \times 10 = 60$
3. $e_B = 13$
4. $e_B \times d_B \equiv 1 \bmod \varphi(n_B)$

   $e_B \times d_B \equiv 1 + (k \times \varphi(n_B))$

   $$d_B = \frac{1 + (k \times \varphi(n_B))}{e_B}$$

   $d_B = ((k \times 60) + 1)/13$

   If $k = 1$, $d_B = 61/13 = 4.69$

   If $k = 2$, $d_B = 121/13 = 9.30$

   If $k = 3$, $d_B = 181/13 = 13.92$

   If $k = 4$, $d_B = 241/13 = 18.53$

   If $k = 5$, $d_B = 301/13 = 23.15$

If $k = 6$, $d_B = 361/13 = 27.76$

If $k = 7$, $d_B = 421/13 = 32.38$

If $k = 8$, $d_B = ((8 \times 60) + 1)/13 = 481/13 = 37$

Plaintext	Decryption	Decryption result	Alphabetic notation
Plaintext (p_1)	46^{37} mod 77	18	s
Plaintext (p_2)	53^{37} mod 77	4	e
Plaintext (p_3)	30^{37} mod 77	2	c
Plaintext (p_4)	69^{37} mod 77	20	u
Plaintext (p_5)	73^{37} mod 77	17	r
Plaintext (p_6)	50^{37} mod 77	8	i
Plaintext (p_7)	61^{37} mod 77	19	t
Plaintext (p_8)	52^{37} mod 77	24	y

plaintext = security