RSA Exercises

RSA and Public Key Codes[1]

1. Find the decoding key *d* for the code whose published values of *N* and *e* are *N* = 233 570 063, *e* = 125.

[d = 136 387 061]

2. Decrypt, by hand, the following RSA-encoded message (*N* = 7387, *e* = 1357):

2133 429 1126

You may assume the following was used to equate letter pairs with 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
11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36

[“NUMBER”]

3. Presume that a plaintext message is converted to a number by making the following substitutions: blank = 99, A=10, B=11, ..., Z=35. Decode, the following message. It is a quotation from Shakespeare's "Hamlet". The coded message consists of four integers:

c_1 = 39 25736 57380 83976

c_2 = 8 66571 70599 56870

c_3 = 14569 39934 49451

c_4 = 14 57541 36754 04137

The public key used for encryption was (*N* = 59 11142 11035 79513, *e* = 123).

RSA Encoding[2]

4. Suppose you want to send a message to a friend. You look up your friends RSA public-key and find that *N* = 1964556481 and *e* = 456899. In blocks of 4 alphabet letters using the ASCII code numerical alphabet assignment, send to your friend the message “THIS IS A SECRET”.

1 The Oxford Math Center, http://www.oxfordmathcenter.com/drupal7/node/206
2 http://www.radford.edu/~npsigmon/courses/cryptography/RSAexercisesSection4.4.doc

Solutions

1. N = 233570063 ⇨ p = 14897 q = 15679 φ(N) = 233539488

   e = 125 ⇨ d = 1/e mod φ(N) = 136387061

2. N = 7387 ⇨ p = 83 q = 89 φ(N) = 7216

   e = 1357 ⇨ d = 1/e mod φ(N) = 5525

   $m_1 = c_1^d \bmod N = 2133^{5525} \bmod 7387 = 2431$ 24 = “N” 31 = “U”

   $m_2 = c_2^d \bmod N = 429^{5525} \bmod 7387 = 2312$ 23 = “M” 12 = “B”

   $m_3 = c_3^d \bmod N = 1126^{5525} \bmod 7387 = 1528$ 15 = “E” 28 = “R” NUMBER