RSA Exercises

RSA and Public Key Codes

Note on RSA Key Length in Educational Exercises: The RSA keys used in these exercises (with values like n=3337 or n=17947) are intentionally small to make calculations manageable by hand. In real-world applications, RSA implementations use much larger keys, typically 2048 or 4096 bits in length (hundreds of digits). These short keys are suitable for learning the mathematical principles behind RSA but would be trivial to break with modern computing power. Production RSA systems require key lengths that make factorization computationally infeasible with current technology.

1. A company uses RSA with parameters p=52 361 and q=75 767. A new employee needs to set up their public key and chooses e=13: a) calculate N and $\varphi(N)$; b) verify if e=13 is a valid choice; c) calculate the private key d.

   [N = 3 967 235 887; $\varphi(N)$ = 3 967 107 760; d = 1 525 810 677]

2. Find the private key d for an RSA cryptosystem with the public key parameters: N = 277 943 821 and e = 101. Show your work.

   [d = 175 918 189]

3. Manually decrypt the following RSA-encrypted message (N = 9 271, e = 1 783):

   7 607 5 284 135

   You may use this conversion table to translate numbers to letters:

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

   [“WORKER”]

4. Consider a plaintext encoding scheme where: *apostrophe* = 98, *space* = 99, A=10, B=11, … , Z=35. Decrypt the following message, which contains a quote from Shakespeare's “*Macbeth*”. The encrypted message consists of four integers:

   c_1 = 44 52776 89172 17514

   c_2 = 16 38084 48977 58847

   c_3 = 19 00433 09400 34049

   c_4 = 24 62874 98943 55566

   The encryption was performed using the public key (N = 63 26552 23557 39019, e = 137).

RSA Encoding

5. You need to transmit a confidential note to a colleague. After retrieving their RSA public key, you find that N = 20757 94951 and e = 2 351. Using 4-letter blocks and the ASCII numerical encoding for letters and spaces, encrypt and send the message “KEEP IT SAFE”.

RSA Cryptography Using Modular Arithmetic Calculator[1]

Exercise: Securing a Digital Message Exchange

In this exercise, you'll implement RSA encryption using the modular arithmetic calculator. You'll work with manageable numbers while still demonstrating all the critical concepts of RSA.

Part 1: Key Generation

(a) Generate two distinct prime numbers:
- Use the “*Utilità*” tab and the prime number functions (NEXT-P, IS-P)
- Select p = 61 and q = 53

(b) Calculate the modulus n:
- Compute $n = p \times q = 61 \times 53 = 3233$
- Enter this value as your modulus (m) in the calculator

(c) Calculate Euler's totient function $\varphi(n)$:
- Use the *(a-1)*(b-1)* function with a = 61, b = 53
- This gives $\varphi(n) = 60 \times 52 = 3120$

(d) Choose a public exponent e:
- Select e = 17
- Verify it's coprime with $\varphi(n)$ using GCD(a,b) function
- Confirm GCD(17, 3120) = 1

(e) Calculate the private exponent d:
- Find d such that $(e \times d) \equiv 1 \pmod{\varphi(n)}$
- Use modular inverse ($1/a$) with a = 17 and m = 3120
- You should get d = 2753

Part 2: Message Encryption and Decryption

(f) Encrypt a sample message:
- Take the message "TOP" with ASCII values T=84, O=79, P=80
- Combine them into a single number: 848079
- Verify this number is less than n (3233)
- Since it's larger, split it: 84, 79, 80

(g) For each number (M), encrypt using:

1 This RSA exercise can be completed using the modular arithmetic calculator available at https://www.netlab.fauser.edu/s/calcmodjs/. The calculator provides all necessary functions including modular exponentiation, GCD calculation, primality testing, and modular inverse calculation, making it an ideal tool for hands-on exploration of RSA principles without requiring manual computation of complex mathematical operations.

- *C* = *M*^*e* mod *n*
- For *M* = 84: *C* = 84^17 mod 3233
- Use the *a*^*b* function on your calculator with proper modulus
- Calculate all three encryptions

(h) Decryption:

- For each ciphertext *C*, compute *M* = *C*^*d* mod *n*
- For example, if *C* = 2557, compute *M* = 2557^2753 mod 3233
- Verify you get back 84, 79, and 80

Solutions

2. N = 277 943 821 ⇨ p = 863 q = 322 067 φ(N) = 277 620 892

   e = 101 ⇨ d = 1/e mod φ(N) = 175 918 189

3. N = 9 271 ⇨ p = 73 q = 127 φ(N) = 9 072

   e = 1 783 ⇨ d = 1/e mod φ(N) = 8 263

   $m_1 = c_1^d \bmod N = (7\,607)^{8\,263} \bmod 7387 = 2431$ 33 = “W” 25 = “O”

   $m_2 = c_2^d \bmod N = (5\,284)^{8\,263} \bmod 7387 = 2821$ 28 = “R” 21 = “K”

   $m_3 = c_3^d \bmod N = (135)^{8\,263} \bmod 7387 = 1528$ 15 = “E” 28 = “R” WORKER