Elementary Number Theory - Exercise 7b

ETH Zürich - Dr. Markus Schwagenscheidt - Spring Term 2023

Problem 1. 1. Choose two 4-digit primes p and q and generate your own public and private RSA keys[1].

2. Exchange your public keys with another student and send each other a (very) short encrypted message[2]. Use the following encoding for the letters:

a	b	c	d	e	f	g	h	i	j	k	l	m
01	02	03	04	05	06	07	08	09	10	11	12	13

n	o	p	q	r	s	t	u	v	w	x	y	z
14	15	16	17	18	19	20	21	22	23	24	25	26

Keep in mind that long messages have to be split into blocks of size less than N.

3. Figure out the private key of your RSA partner.

Problem 2. Let $N = pq$ be a product of two odd primes, and $\varphi(N) = (p-1)(q-1)$. Show that p and q can quickly be computed if N and $\varphi(N)$ are known.

For example, given $N = 7261$ and $\varphi(N) = 7072$, compute p and q.

Problem 3. Let $N = pq$ be a product of two odd primes. If p and q are too close, then N can quickly be factored, using *Fermat's factorization method*: the idea is to find a, b with $N = a^2 - b^2$, since then $N = (a-b)(a+b) = pq$ is a factorization of N. If p, q are close, then b will be relatively small, so a will roughly be equal to $\sqrt{N}$. Here's the algorithm:

Compute $a = \lceil\sqrt{N}\rceil, \lceil\sqrt{N}\rceil + 1, \lceil\sqrt{N}\rceil + 2, \dots$ until $a^2 - N = b^2$ is a square. Then $N = (a-b)(a+b)$ is a factorization of N.

Show that Fermat's method will always find a factorization of $N = pq$, and use it to factor $N = 5959$.

Problem 4. Let $N = pq$, where p is an odd prime, but q is a *Carmichael number* with $\gcd(p, q) = 1$. Show that the RSA encryption and decryption still works on messages m with $\gcd(m, N) = 1$.

Problem 5. In cryptographic applications, it is often important to keep computation costs low. Hence, it is common to use rather small public keys e to speed up the RSA encryption. A typical choice is $e = 3$, since the encryption then takes only 2 multiplications. Here we discuss two attacks on RSA with $e = 3$.

[1] You could ask Wolframalpha for random 4-digit primes.

[2] Use Wolframalpha for the necessary computations.

1. Bob uses the public key $e = 3$ and the modulus $N = 126589$. Alice sends the encrypted message $c = 3375$ to Bob. Can you decrypt the message (without factoring N)?

2. Bob, Charles, and Dora all use the same public key $e = 3$, but with different moduli N_B, N_C, N_D. Let us assume that N_B, N_C, N_D are pairwise coprime[3]. Alice sends the same message m to Bob, Charles, and Dora, encrypted as c_B, c_C, c_D with their respective public keys and moduli. Use the Chinese Remainder Theorem to explain how m can be decrypted, without factoring any of the moduli.

Problem 6 (sage)**.** 1. Implement the RSA key generation and encryption/decryption. You could ask the user for primes p and q, or offer random primes.

2. Implement Fermat's factorization method, and factor $N = 105327569$.

[3]Bonus question: how can we break RSA if N_B, N_C, N_D are not pairwise coprime?