Cryptography & Encryption:6G7Z1011: Lab Questions

Keith Yates

March 1, 2019

Cryptography & Encryption:6G7Z1011 : The RSA Algorithm

1 Cryptography & Encryption:6G7Z1011 : The RSA Algorithm

We discuss the most widely used public key encryption algorithm

1.1 the RSA algorithm

The usual notation is in place: for example, $K_{B,Pr}$ is a key belonging to Bob and it is private, and $K_{B,Pu}$ is a key belonging to Alice and it is public, and p, q are prime numbers.

1. Bob picks two primes p and q (p, $q > 2^{1000}$) evaluates $N = pq$ and picks an encryption exponent e, where e satisfies
$$\gcd(e, (p-1)(q-1)) = 1. \tag{1}$$
2. Bob's public key is the tuple (that is, it is a pair of numbers) $K_{B,Pu} = (N, e)$
3. Alice has a plaintext message m (m an integer) and evaluates
$$c = m^e \mod N, \tag{2}$$
c is the ciphertext sent to Bob.
4. Bob solves
$$ed = 1 \mod (p-1)(q-1). \tag{3}$$
The only term in eqn. 3 that Bob does not know is d.
5. Bob evaluates
$$m' = c^d \mod N \tag{4}$$
and we find $m = m'$.

2 Problems & Supplementary Material:Problems

2.1 problem:

⌜Consider the field $\mathbb{F}_{17}$ then $\mathbb{F}_{17}^*$ is a group of order 16.

1. Using JAVA determine the subgroups generated by each single element of $\mathbb{F}_{17}^*$ and in each case verify that the order of the group generated by the element divides 16.
2. Recall those elements of $\mathbb{F}_{17}^*$ that generate the entire group are termed primitive; what are the primitive elements of $\mathbb{F}_{17}^*$. Hint : 2 is not a primitive root, but 3 is a primitive root.

⌟

2.2 problem:

⌜Write Java code that implements the RSA algorithm, check it works by running it with the following data.

1. Let Bob pick two primes $p = 1223$ and $q = 1987$, what is the value of $N = pq$. [Answer: $pq = 2430101$.]
2. Bob picks an exponent $e = 948047$, check that $\gcd(e, (p-1)(q-1)) = 1$ and his public key is the tuple $K_{B,Pu} = (N, e)$
3. Alice's plaintext message is $m = 1070777$
4. Alice encrpyts m to
$$c = m^e \mod N; \tag{5}$$
c is sent to Bob.
5. Bob solves for d in
$$ed = 1 \mod (p-1)(q-1) \tag{6}$$
6. Bob evaluates
$$m'c^d \mod N \tag{7}$$
and,if it has all worked, $m = m'$

⌟

2.3 problem:Lagrange

⌜ Let S_3 denote the permutation group on three objects, and let $H = \langle(1,2,3)\rangle$ denote the subgroup generated by the permutation $(1,2,3)$. Find a decomposition of S_3 into cosets of the form $G = \sqcup_{a \in G'} Ha$ where G' is some subset of G.
⌟

2.4 problem:Properties of ϕ

To get you thinking.

1. What is $\phi(p)$ for p prime?
2. Prove $\phi(p^i) = p^{i-1}(p-1)$
3. Verify directly $\phi(15) = \phi(3)\phi(5)$

2.5 problem:

⌜Consider $\mathbb{F}_2 = \{0, 1\}$ and let $GL(2, \mathbb{F}_2)$ denote the set of invertible matrices of size 2×2 with entries from $\mathbb{F}_2$. Show that $GL(2, \mathbb{F}_2)$ is a group. $GL(2, \mathbb{F}_2)$ is isomorphic to a group we have meet before — which one?
⌟

2.6 problem:primes

⌜ The RSA algorithm depends on certain properties of the primes. Answer the following questions:

1. Are there an infinite number of primes? If you think there are can you prove it?
2. A prime of the form $2^n - 1$ is called a *Mersenne prime*, for $1 \leq n \leq 10$ determine if $2^n - 1$ is prime.
3. Are there an infinite number of Mersenne primes?
4. If n is even and $n > 2$ prove $2^n - 1$ is not prime.
5. If $3 \mid n$ and $n > 3$ then prove $2^n - 1$ is not prime.

⌟

2.7 problem:

⌜Continue with your assignment. ⌟