Public Key Encryption: The RSA Algorithm

Lynne Chervitch, Jillian Gaietto, Jessica Pugliese
Advisor: Dr. Gang Yu, Professor of Mathematics, Kent State University

Abstract
Over the past decade, the frequency and sophistication of intrusions into U.S. government, private industries and personal databases has grown exponentially. As the cyber threat landscape continues to evolve, it is becoming increasingly important to understand and implement effective security measures.

Resources: The working with government agencies. Our combined knowledge protects our information technology national security, the need for layered and databases has grown exponentially. As the “secret” number d, 1<d<φ(n), satisfying φ(n) are relatively prime).

RSA Encryption in Action
(example provided by Dr. Gang Yu, Professor of Mathematics, Kent State University)

We need to let the letters of the alphabet be denoted by numbers, i.e., 00 – “Blank”; 01 – “A”, 02 – “B”, …, 26 – “Z”.

Recently, Alice and Bob have been sending messages to each other using the RSA Algorithm. Their public key is n=338,699 and e=77,893, and only Bob knows that m^e=43, and p=577, and q=857. Therefore, Alice was accepted to graduate school and Bob asked what school Alice would be attending. Since this would not yield 01231402 as we are dealing with integers.

Using the Euclidean Algorithm we will find our number d satisfying d≡e⁻¹ (mod φ(n)).

Hence, 1 = 13a − 3b (and equivalently, 13a = 3b + 1).

So d = 13.

3) Our message C=223,208 can be written

C≡m^e (mod n)

Thus:
C = (223,208^d)≡m^e (mod n)

Therefore, M = 23,228,094 (mod 338,699)

Using our alphabet we can read this as: 27,877 = A

It is not hard to verify that these numbers satisfy the condition, we can write:

Claim: (m^e)^d≡m (mod n).

Therefore, Alice will be attending USC for graduate school.

Appplied Proof
To define the RSA Algorithm as a general cryptographic system, there must be a general proof for any message m that must be encrypted.

Suppose: gcd(c,d)=1  Npq ed−1 mod(N)

Claim: (m^d)^e≡m (mod N)

Proof: Being m e 2n there are only two possible cases to analyze:

1) gcd(N, d) = 1
   In this case Euler’s Theorem stands, assuming that m^d≡m (mod N), As for the claim to prove, because of the third condition, we write: m^d≡m (mod N).
   Furthermore, m^{ed−1}≡m (mod N), by Euler’s theorem m^{ed−1}≡m (mod N).

   Therefore, Alice will be attending USC for graduate school.

Setting Up the Algorithm

Step 1. We need to have 2 large distinct prime numbers. We call these p and q.

Step 2. We find p^q and q^p.

Step 4. We need to choose an integer e, 1<e<q (such that gcd(e,q)=1 (i.e. e and q are relatively prime)).

Then we have: (n,e) as the public key and (d,p,q) as the private information.

When we put RSA Encryption into action, we will also denote the message that needs encoded as:

C≡M^e (mod n)

where C is the encrypted number and M is the message we are trying to recover.

RSA Encryption’s Creators

Above: Padlock icon from the Firefox Web browser, which indicates that TLS, a public-key cryptography system, is in use.

Left: RSA encryption is used today by constantly switching security keys on devices.