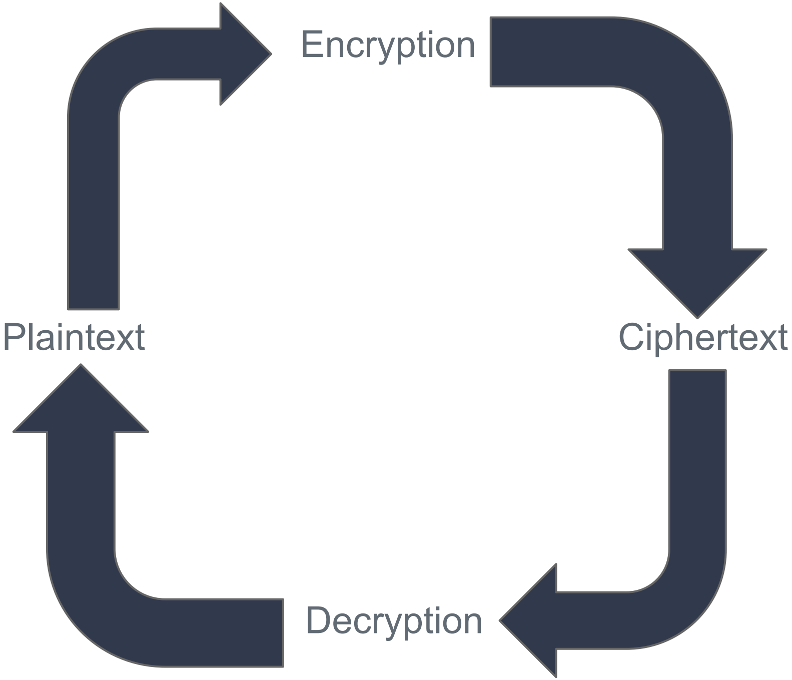
A Brief Introduction to RSA Encryption

Riley Guyett

The Basic Idea



Two types of keys

1) Private key – Encryption (f) and decryption (f^{-1}) come from the same function. f and f^{-1} must be easy to compute, but hard to guess
   a) Both sender and receiver know f and f^{-1}
2) Public key – Encryption and decryption come from different functions. f must be easy to compute, but f^{-1} must be hard to compute without extra information
   a) Both sender and receiver know f, but only receiver knows f^{-1}

RSA Encryption — Theory

It is relatively easy to find 2 large primes and multiply them together

However, it is much, much harder to factor that product into those 2 large primes

If there was an encryption key based on the product of the primes, and a decryption key based on the primes themselves, one could make a public key cryptography system

RSA Encryption — Setup

1) Take 2 large random primes p,q (say, 150-digits each)
2) Compute n=pq and m=(p-1)(q-1)
3) Find E such that gcd(E,m)=1
4) Find D such that DE ≡ 1 (mod m)
5) Publish E and n, and keep D and m private

If people want to send you a message x, they send you

$$y=x^E \pmod n$$

If you want to recover the encrypted message, compute

$$x=y^D \pmod n$$

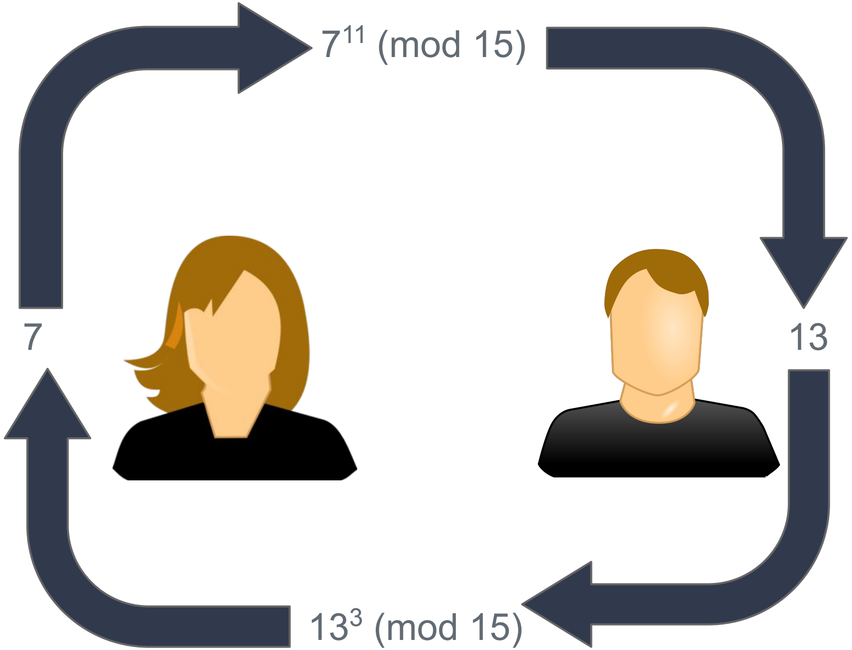
Example

Let p=3 and q=5. Then n=15 and m=8. Let E=11 and D=3.

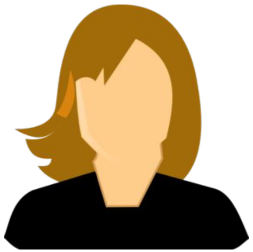
Alice wants send Bob the plaintext “7” using this method. Using their encryption method, $y=x^E$ (mod n) $=7^{11}$ (mod 15) =13, so she send Bob the ciphertext 13.

Bob then decrypts the ciphertext as $x=y^D$ (mod n) $=13^3$ (mod 15) =7

In general, you can send any number as a plaintext, but it’s better to send a few digits at a time to make computation easier and to break up the message (more security)

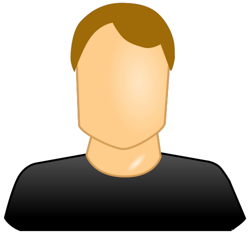


RSA — Sender Verification



g

g^{-1}



f

f^{-1}

How does Bob know that Alice sent him that message. Since anyone can make a ciphertext, he has no way of knowing that he message is from Alice just by looking at it.

But what if Alice had her own RSA encryption key g and decryption key g^{-1}? If she tells Bob her encryption key, now both of them can verify that they are talking to each other using the following method:

Alice sends $y=f(g^{-1}(x))$ to Bob. Bob then decrypts the message using $g(f^{-1}(y))= g(f^{-1}(f(g^{-1}(x))))=g(g^{-1}(x))=x$. Since only Alice knows g^{-1}, Bob knows that this message came from her.

Thank You!