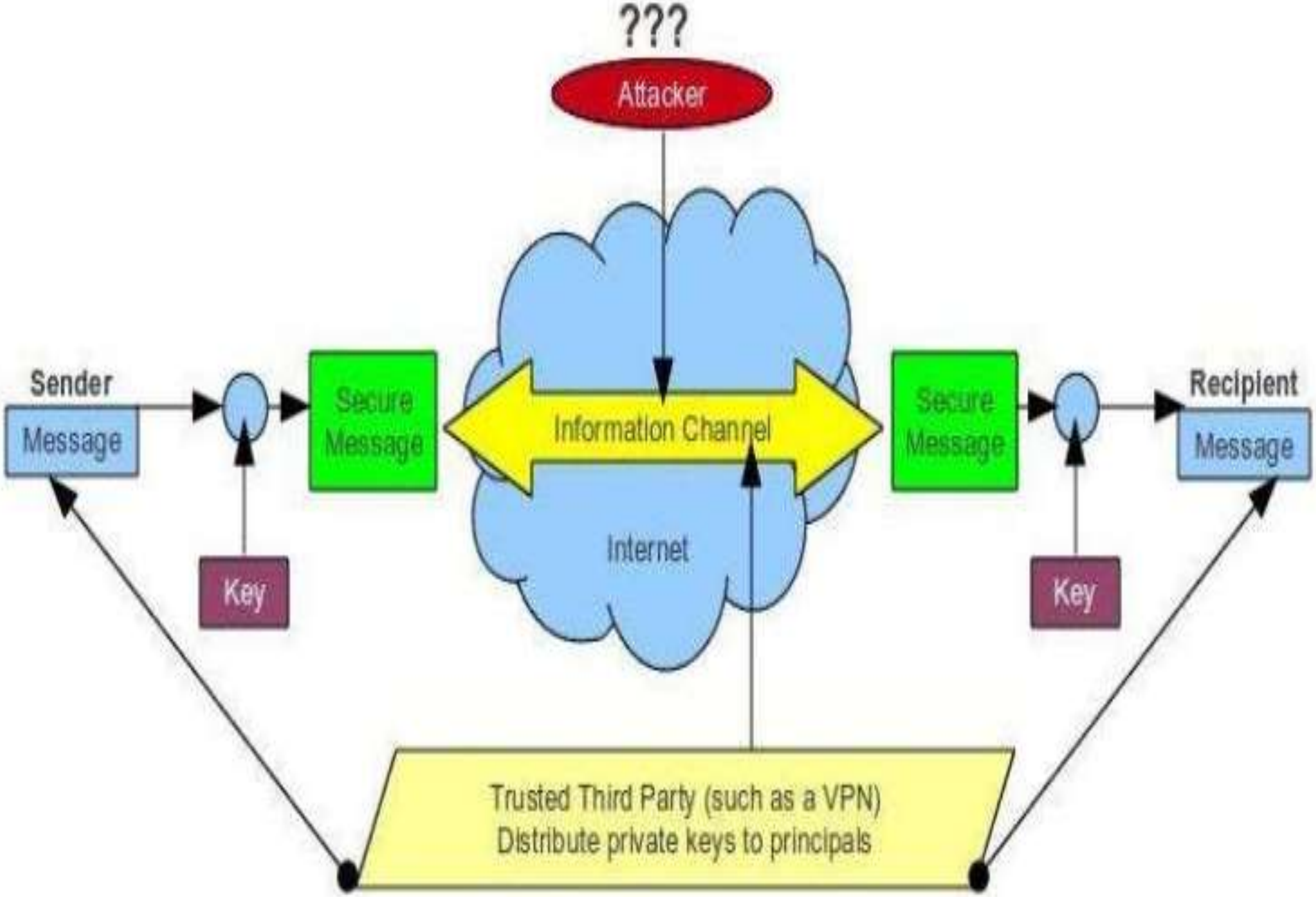
What is Cryptography?

- Cryptography is the practice and study of techniques for conveying information security.
- The goal of Cryptography is to allow the intended recipients of the message to receive the message securely.

Cryptography and network security

- Network security is one of the several models of security which exist today. This is most efficient and widely used model.
- Here the focus is to control network access to various hosts and their services, rather than controlling individual host security.
- Hence, modern cryptography techniques are implemented in the Network Security Model, as it proves to be affordable, functional and reliable.



Elementary Network Security Model

Important Terms

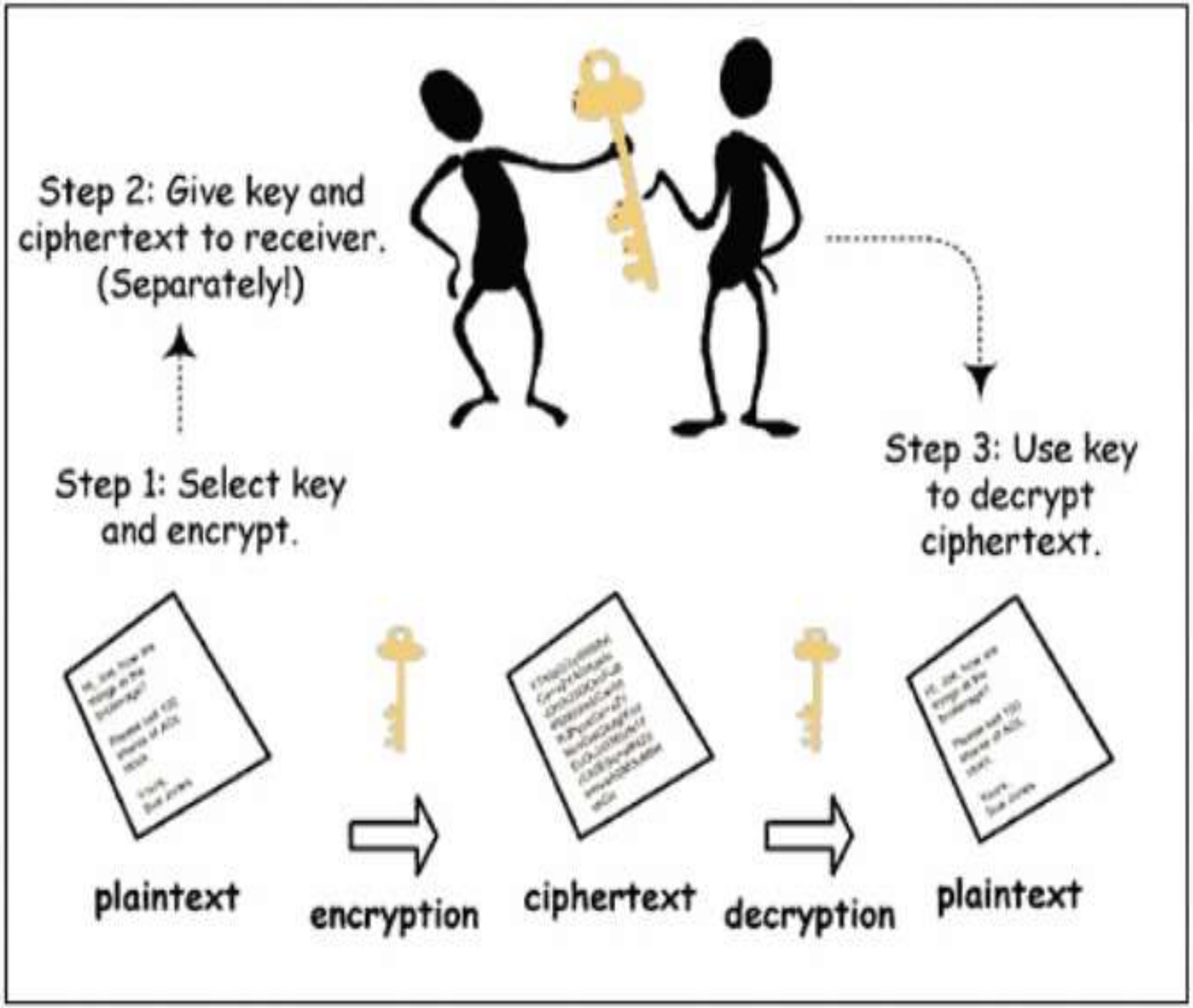
- Plaintext – The message in its original form.
- Ciphertext – Message altered to be unreadable by anyone except the intended recipients.
- Cipher- The algorithm used to encrypt the message.
- Cryptosystem – The combination of algorithm, key, and key management functions used to perform cryptographic operations.

Types of cryptography

- Private-key cryptography or Symmetric-key algorithm
- Public-key cryptography or Asymmetric-key algorithms

Private Key Cryptography

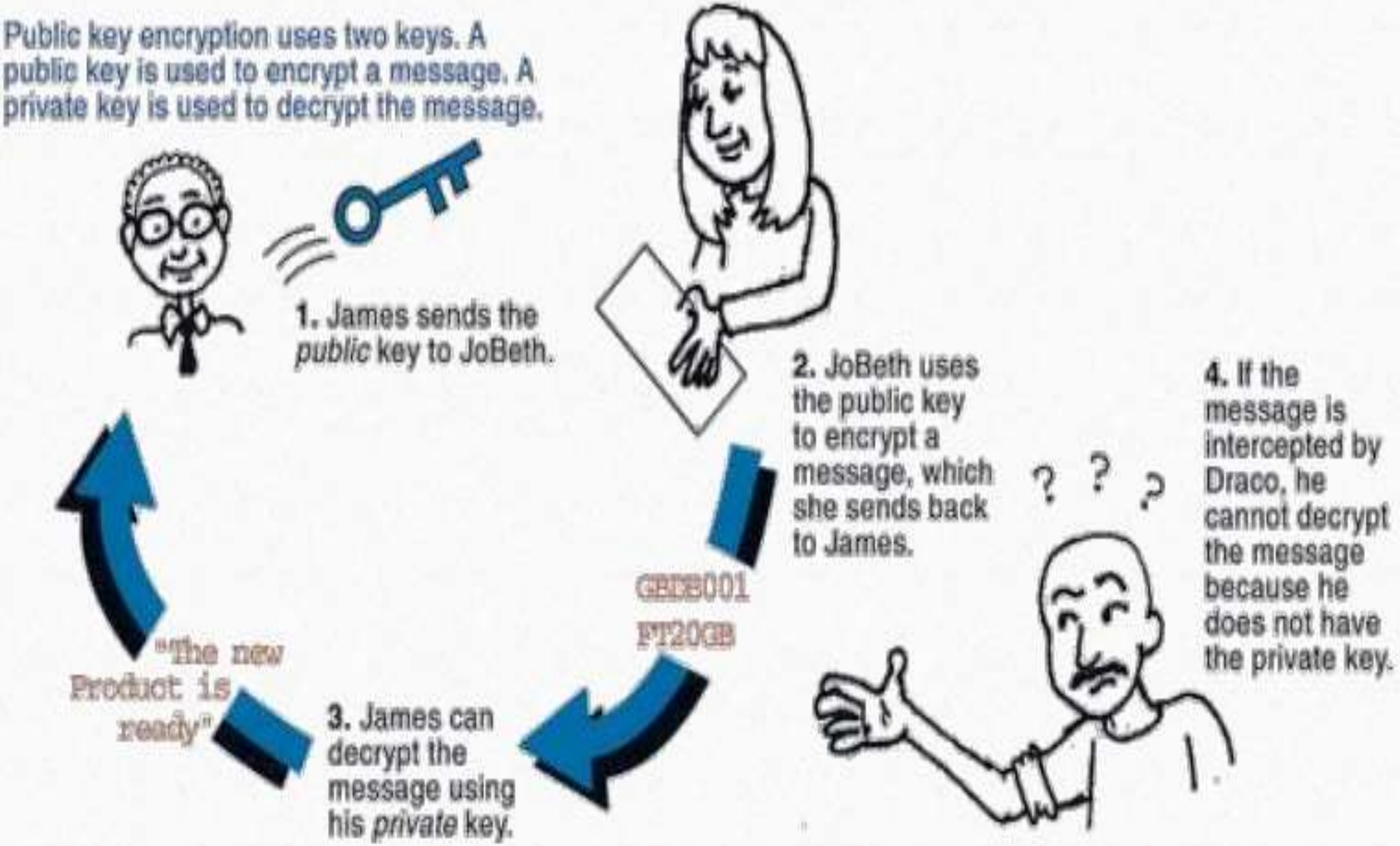
- A single key is used for both encryption and decryption. That's why its called “symmetric” key as well.
- The sender uses the key to encrypt the plain-text and the receiver applies the same key to decrypt the message.
- The biggest difficulty with this approach, thus, is the distribution of the key, which generally a trusted third-party VPN does.


Step 2: Give key and ciphertext to receiver. (Separately!)
Step 1: Select key and encrypt.
Step 3: Use key to decrypt ciphertext.
plaintext
encryption
ciphertext
decryption
plaintext

Schematic representation of Private-key cryptography

Public-Key Cryptography

- Each user has a pair of keys: a public key and a private key.
- The public key is used for encryption. This is released in public.
- The private key is used for decryption. This is known to the owner only.



Public key encryption uses two keys. A public key is used to encrypt a message. A private key is used to decrypt the message.

1. James sends the *public* key to JoBeth.

2. JoBeth uses the public key to encrypt a message, which she sends back to James.

3. James can decrypt the message using his *private* key.

4. If the message is intercepted by Draco, he cannot decrypt the message because he does not have the private key.

Schematic representation of Public-key cryptography

RSA CRYPTOSYSTEM

- The most famous algorithm used today is RSA algorithm.
- It is a public key cryptosystem developed in 1976 by MIT mathematicians - Ronald Rivest, Adi Shamir, and Leonard Adleman.
- RSA today is used in hundreds of software products and can be used for digital signatures, or encryption of small blocks of data.

Mathematical Prerequisites

- Euclid's Algorithm and its extension
- Modulo operator, its congruence, and multiplicative inverse
- Euler's Phi Function and Theorem

Euclid's Algorithm

- It is a method of computing Greatest Common Divisor of two integers (generally positive) .
- It is based on two observations :

a) If a perfectly divides b, then GCD(a,b) = a

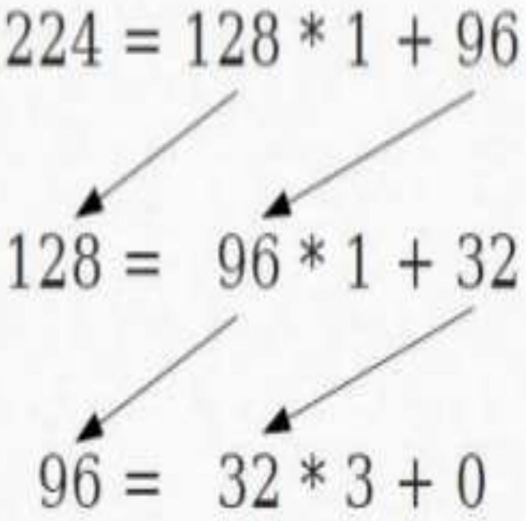
b) If a = b * t + l where t and l are integers, then

GCD(a,b) = GCD(b,l)

- It is applied in chain until the remainder is zero.

Example

Suppose we are looking for ***GCD(224,128)*** :



224 = 128 * 1 + 96 *(a=224, b=128, l=96)*

128 = 96 * 1 + 32 *(a=128, b=96, l=32)*

96 = 32 * 3 + 0 *(a=96, b=32, l=0)*

Hence, ***GCD(224,128)*** is ***32***

Modulo Arithmetic

- The modulo operation finds the remainder of division of one number by another.
- For example, 14 mod 12 = 2 , as when 14 is divided by 12 we get the remainder as 2.

Modulo Arithmetic

- The modular congruence, indicated by "≡" followed by "mod" between parentheses, means that the operator "mod", applied to both members, gives the same result.
- For example, 38 ≡ 14 (mod 12) is same as 38 mod 12 = 14 mod 12 , which both yield 2.

Modulo Arithmetic

- The modular multiplicative inverse of a mod m is an integer x such that a*x ≡ 1 (mod m)
- For example, we wish to find modular multiplicative inverse x of 3 mod 11. We can write this as
- $3^{-1} \equiv x \pmod{11}$ which is same as $3^*x \equiv 1 \pmod{11}$
- Since RHS is 1, we need to find x such that (3*x) mod 11 = 1 which would give minimum positive value of x as 4.

Extended Euclid's Algorithm

- The Extended Euclid's Algorithm computes the integers x and y in the equation called Bézout's identity which is :

$$ax + by = GCD(a,b)$$

- When a and b are co-primes, x is given as $a-1 \equiv x \pmod{b}$ and y is given as $b-1 \equiv y \pmod{a}$
- Hence we can easily find out the modular multiplicative inverse this way.

Euler's Theorem

- Euler's Theorem states that if GCD (a,n)=1, i.e., a and n are co-primes, then $a\varphi(n) \equiv 1 \ (\mathrm{mod}\ n)$
- If n is prime, then we have $an-1 \equiv 1 \ (\mathrm{mod}\ n)$
- If n is the product of two primes p and q, then $a(p-1)^{*}(q-1) \equiv 1 \ (\mathrm{mod}\ n)$.

This concept forms the basis of encryption process in RSA cryptosystem.

Setting up RSA Cryptosystem

ALGORITHM

1. A user must first choose two large prime numbers, say p and q

EXAMPLE

1.Let Alice choose p=11 and q=19.

Setting up RSA Cryptosystem

ALGORITHM

2.Calculate n = p * q

EXAMPLE

2.Alice calculated p * q as 11 * 19 and got the value of n = 209.

Setting up RSA Cryptosystem

ALGORITHM

3.Calculate $\varphi(n) = (p-1) * (q-1)$

EXAMPLE

3.Alice calculated $(p-1) * (q-1)$ as $10 * 18$ and got the value of $\varphi(n) = 180$.

Setting up RSA Cryptosystem

ALGORITHM

4.Choose a value of e such that $GCD(e,\varphi(n)) = 1$.

EXAMPLE

4.Alice randomly chose e as 103 which is co-prime to 180.

Setting up RSA Cryptosystem

ALGORITHM

5.Calculate d such that $e * d \equiv 1 \pmod{\varphi(n)}$, or in other words, find the modular multiplicative inverse of e.

EXAMPLE

5.To find the required inverse, Alice would use Euclid's Algorithm in reverse manner and then use its extension to find the inverse. Here's how:

Setting up RSA Cryptosystem

- Applying Euclid's:

180 = 1 * 103 + 77

103 = 1 * 77 + 26

77 = 2 * 26 + 25

26 = 1 * 25 + 1

Remember, Alice chose e = 103 and φ(n) = 180

Setting up RSA Cryptosystem

- Finding Inverse:

We now write our Bézout's Identity as $ex + \varphi(n)y = 1$, and we just determined x as 7.

Now, the inverse of e is e-1$\equiv x \pmod{\varphi(n)} \equiv 7 \pmod{180}$

Hence, $d = 7$

Setting up RSA Cryptosystem

ALGORITHM

6.The Public keys are (e,n),

7.The Private keys are (d,n) .

EXAMPLE

6.Alice thus obtained her Public Key as (103,209) and Private Key as (7, 209)

Encryption Process

ALGORITHM

In order to encrypt a number m, we calculate $c \equiv me$ (mod n), where c is the encrypted number and m is less than n, keeping in mind that the encryption (public) key is (e,n).

EXAMPLE

Bob wants to send Alice and important number, say 10. The cipher using Alice's public key would be $c \equiv 10103$ (mod 209)

On calculating this, which comes out to be 32, Bob sends it to Alice.

Decryption Process

ALGORITHM

In order to decrypt a cipher c, we calculate $m \equiv cd \pmod{n}$, where m is the original number, keeping in mind that the decryption (private) key is (d,n) .

EXAMPLE

Alice receives the encrypted number. The decrypted number using her private key would be $m \equiv 32\ 7 \pmod{209}$

On calculating this, she gets m=10, which was desired.

RSA Algorithm

Key Generation

Select p, q	p and q both prime
Calculate n	$n = p \times q$
Select integer d	$gcd(\phi(n), d) = 1;\ 1 < d < \phi(n)$
Calculate e	$e = d^{-1} \bmod \phi(n)$
Public Key	$\mathrm{KU} = \{e, n\}$
Private Key	$\mathrm{KR} = \{d, n\}$

RSA Algorithm

Encryption

- Plaintext: $M < n$
- Ciphertext: $C = M^e \pmod{n}$

Decryption

- Ciphertext: C
- Plaintext: $M = C^d \pmod{n}$

RSA Example

- $p = 3$
- $q = 11$
- $n = p \times q = 33$ -- This is the *modulus*
- $z = (p\text{-}1) \times (q\ \text{-}1) = 20$ -- This is the totient function $\phi(n)$. There are 20 relative primes to 33. What are they? 1, 2, 4, 5, 7, 8, 10, 13, 14, 16, 17, 19, 20, 23, 25, 26, 28, 29, 31, 32
- $d = 7$ -- 7 and 20 have no common factors but 1
- $7e = 1 \bmod 20$
- $e = 3$
- $C = M^e \pmod{n}$
- $M = C^d \pmod{n}$

RSA Weaknesses

- At present, 512 bit keys are considered weak, 1024 bit keys are probably secure enough for most purposes, and 2048 bit keys are likely to remain secure for decades.
- One should know that RSA is very vulnerable to **chosen plaintext attacks**. There is also a new **timing attack** that can be used to break many implementations of RSA.
- The RSA algorithm is believed to be safe when used properly, but one must be very careful when using it to avoid these attacks.

Attacks Against RSA

- Brute Force
  - Try all possible keys
- Mathematical Attacks
  - Factor n
  - Calculate $\phi(n)$
- Timings Attacks
  - Use the running time of the algorithm to determine d, the decryption key

Conclusion

The RSA Cryptosystem is perhaps the most beautiful application of mathematics. Theorems of Euler and Euclid we discussed were proved around 300 years ago, and we find it's application today extensively in network security, computer software algorithms and in further advancement of technology to create a better world.