Cryptography and Network Security

(Professional Elective-I)

Course Objectives

- Acquire fundamental knowledge on the concepts of :

  -Number theory,

  -Cryptographic techniques,

  -Hash functions,

  -Digital signature and

  -Cryptanalysis.

Course Outcomes

1. Describe basics of number theory.
2. Explain various Cryptographic Techniques and ciphers.
3. Describe the different types of asymmetric ciphers.
4. Understand the cryptographic hash functions.
5. Describe about cryptanalysis.

Syllabus

- **UNIT-I:**
- **Introduction to cryptography, Number Theory:** Divisibility and the Division Algorithm, The Euclidean Algorithm, Modular Arithmetic, Prime Numbers, Fermat's and Euler's Theorems,Testing for Primality.
- **Security Concepts:** Introduction, The need for security, Security
- Approaches ,Principles of security, Types of Security attacks, Security
- services, Security Mechanisms, A model for Network Security.
- UNIT-II:
- **Symmetric Ciphers:** Symmetric Cipher Model, Classical Encryption
- Techniques, Substitution Techniques ,Transposition Techniques.
- **Block Ciphers:** Traditional Block Cipher Structure, Block Cipher Design Principles. Block Cipher Modes of Operation. DES, The Strength of DES, Triple DES.
- **Advanced Encryption Standard:** AES Structure ,AES Transformation Functions , Stream Ciphers.

- **UNIT-III:**
- **Asymmetric Ciphers:** Public-Key Cryptography and RSA - Principles of Public-Key Cryptosystems, The RSA Algorithm .
- **Other Public-Key Cryptosystems :** Diffie-Hellman Key Exchange,
- ElGamal Cryptographic System, Elliptic Curve Arithmetic, Elliptic Curve Cryptography
- UNIT-IV:
- **Cryptographic Hash Functions :** Applications of Cryptographic Hash Functions, MD5, Secure Hash Algorithm (SHA),SHA-3.
- **Message Authentication Codes :** Message Authentication
- Requirements. Message Authentication Functions, MACs Based on Hash Functions: HMAC MACs Based on Block Ciphers: CMAC, Digital
- Signatures.
- UNIT-V:
- **Cryptanalysis:** Introduction, Time-Memory Trade-off Attack,
- Differential and Linear Cryptanalysis. Cryptanalysis on Stream Cipher,
- Modern Stream Ciphers, Shamir's secret sharing, Identity-based
- Encryption (IBE), Attribute-based Encryption (ABE).

Text Books

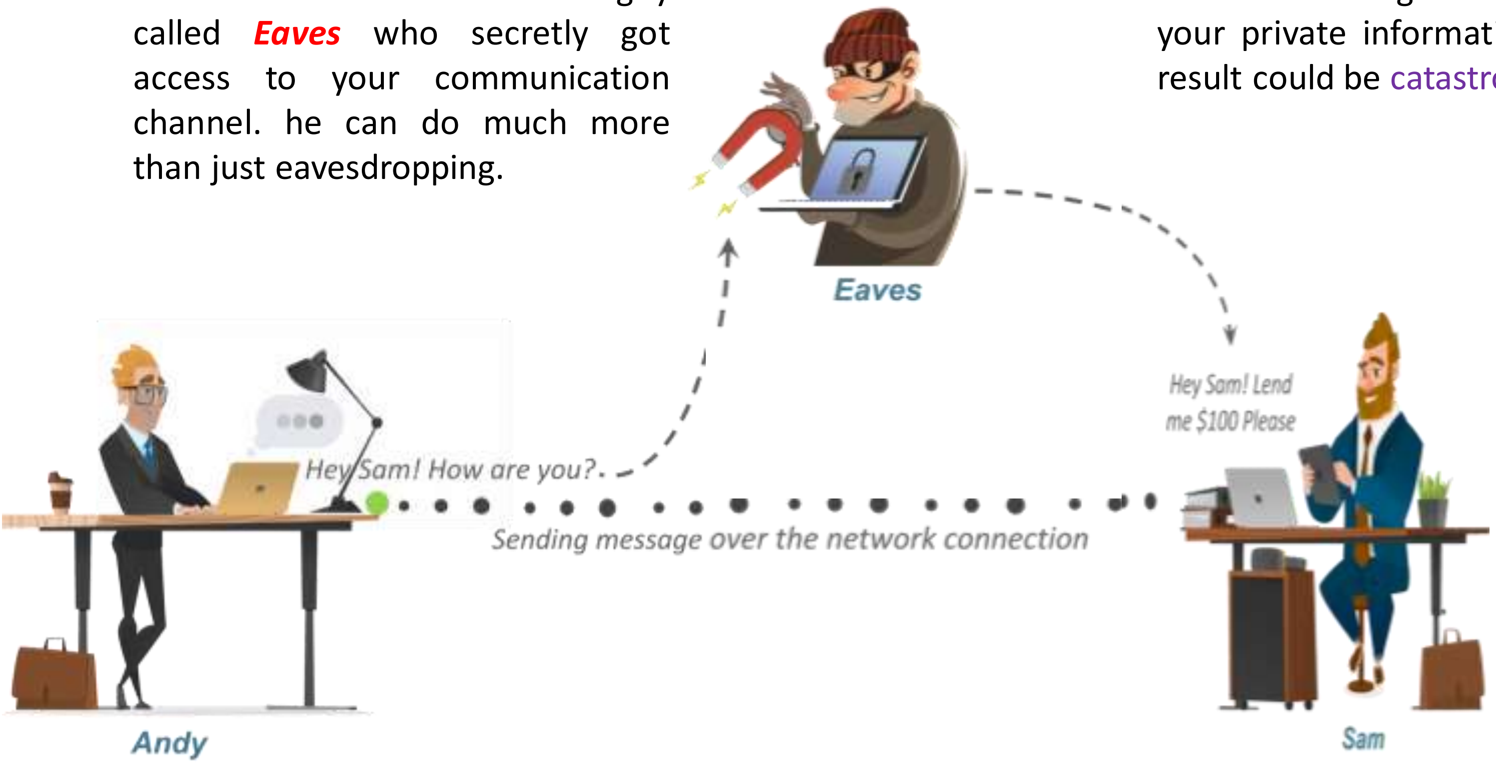
- William Stallings, Cryptography and Network Security, 7th Edition, Pearson Education,2017.
- Behrouz A. Ferouzan, “Cryptography & Network Security”, Tata Mc Graw Hill, 2007.

Introduction

- Cryptography,
- Number Theory,
- Network Security.

There is a smart guy called ***Eaves*** who secretly got access to your communication channel. he can do much more than just eavesdropping.

What if *Eave* gets access to your private information? The result could be catastrophic.



Message to be private and nobody else should have access to the message.
The main goal is to secure this communication.

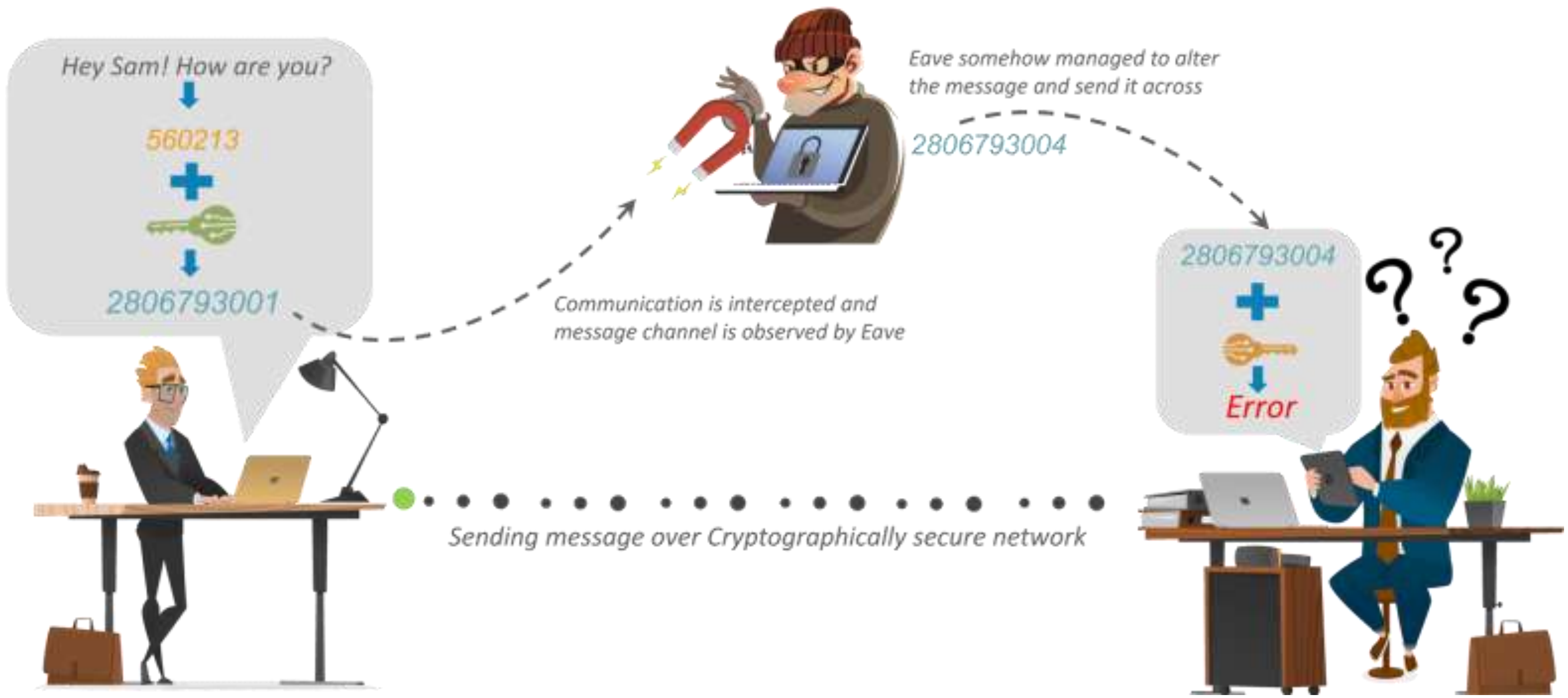
So how can *Andy* be sure that nobody in the middle could access the message sent to *Sam*?

That's where ***Encryption or Cryptography*** comes in.

What Is Cryptography?

- **Cryptography** is the practice and study of techniques for securing communication and data in the presence of adversaries.
- *let's see how cryptography can help secure the connection between Andy and Sam.*

The term Cryptography is derived from the Greek word *kryptos,* which means hidden. It is closely associated to encryption, which is the act of scrambling ordinary text into what's known as ciphertext and then back again upon arrival.



Andy won't have to worry about somebody in the middle of discovering his private messages.

Now, **this error is very important**. It is the way *Sam* knows that message sent by *Andy* is not the same as the message that he received.

Thus, we can say that encryption is important to communicate or share information over the network.

- Cryptography can reformat and transform our data, making it safer on its trip between computers.
- ***Cryptography*** is the science of using mathematics to encrypt and decrypt data.
- The technology is based on the essentials of secret codes, augmented by modern mathematics that protects our data in powerful ways.

Introduction to Number Theory

We will also learn some basics of Number Theory. It is required to understand the mathematical background of various cryptographic techniques.

Number theory is present in every part of cryptographic algorithms. Perform operations on "numbers".

some elementary concepts in number theory are very central to the field of the cryptology

- Understand the concept of divisibility and the division algorithm.

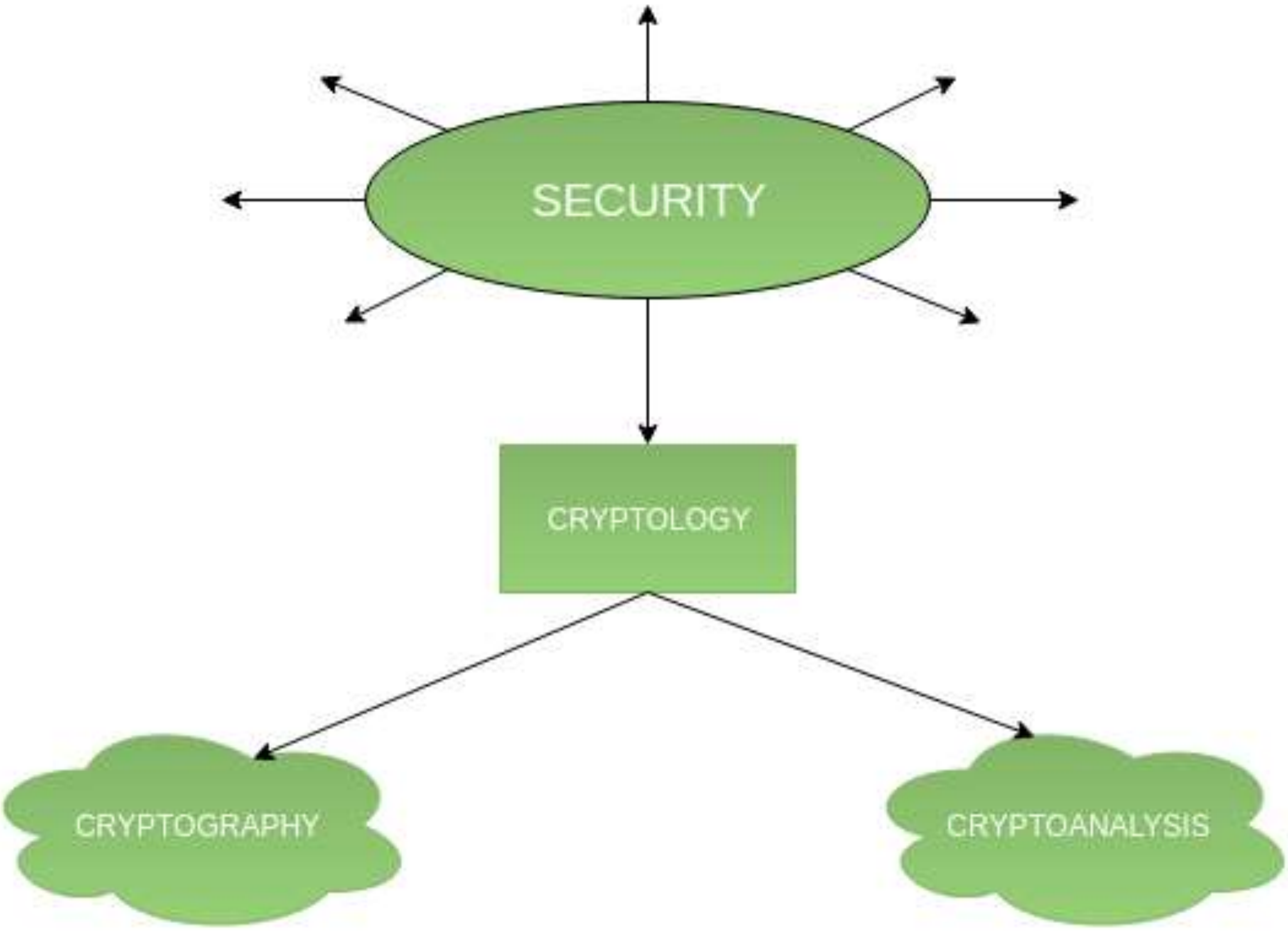
- Understand how to use the Euclidean algorithm to find the greatest common divisor.

- Present an overview of the concepts of modular arithmetic.

- Discuss key concepts relating to prime numbers.

- Understand Fermat's and Euler's theorem.

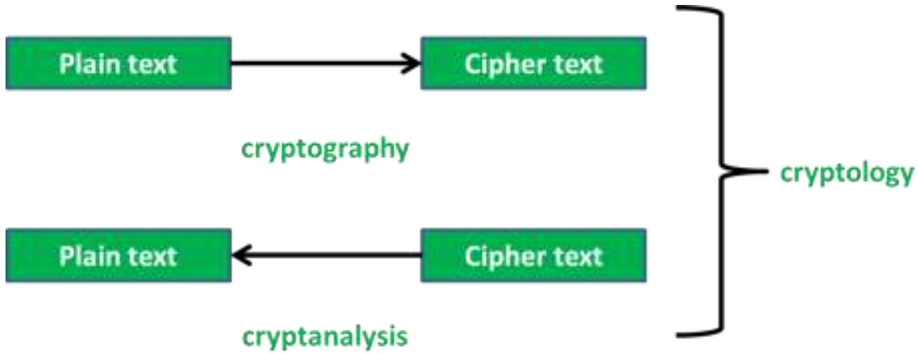
- Make a presentation on the topic of testing for primality.



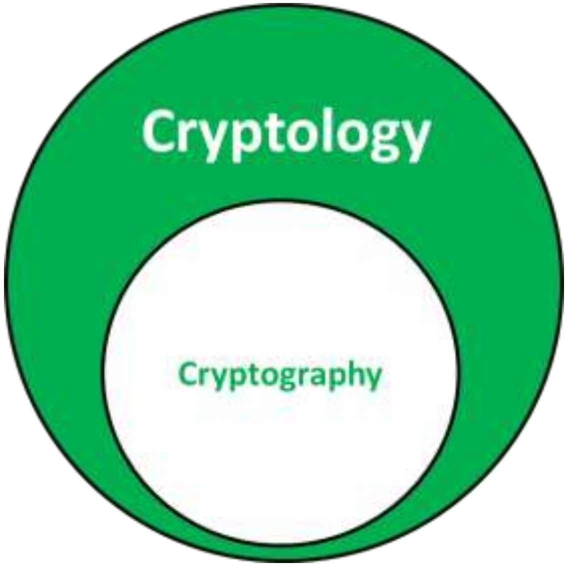
While **cryptography** is the science of securing data, **cryptanalysis** is the science of analyzing and breaking secure communication.

Difference between Cryptography and Cryptology

- **Cryptography** is the study of conversion of plain text(readable format) to ciphertext(non-readable format) i.e. encryption. It is also called the **study of encryption**.
- **Cryptology**, on the other hand, is the study of the conversion of plain text to ciphertext and vice versa. It is also called the **study of encryption and decryption**.



One major difference is that Cryptology is the parent of Cryptography.



Cryptography	Cryptology
Cryptography is the process of conversion of plain text to cipher text.	Cryptology Is the process of conversion of plain text to cipher text and vice versa.
It is also called the study of encryption	It is also called the study of encryption and decryption.
It takes place on the sender side	It takes place on the sender and receiver side
In Cryptography, sender sends the message to receiver.	In Cryptology, both sender and receiver send messages to each other.
Cryptography can be seen as the child of Cryptology	Cryptology can be seen as the parent of Cryptography

Thank You

Network Security

- Security **means safety**, as well as the measures taken to be safe or protected.

- The goal of security is **to protect the assets, devices and services from being stolen or exploited/broken by unauthorized users.**

- Security is therefore the process for ensuring our safety.

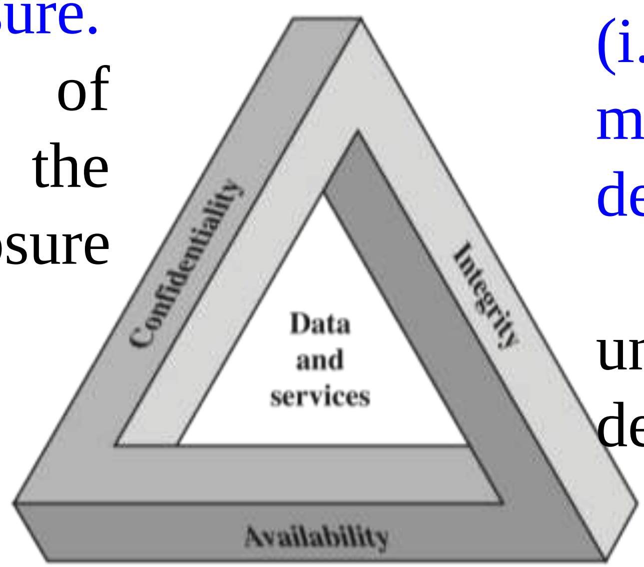
- Security is defined as being free from danger, or feeling safe.

- An example of security is **when you are at home with the doors locked and you feel safe**. Freedom from doubt, anxiety, or fear; confidence. ... If you see an intruder, call security.

Goals of Security-CIA triad

Confidentiality: The protection of data from unauthorized disclosure.

A loss of confidentiality is the unauthorized disclosure of information.



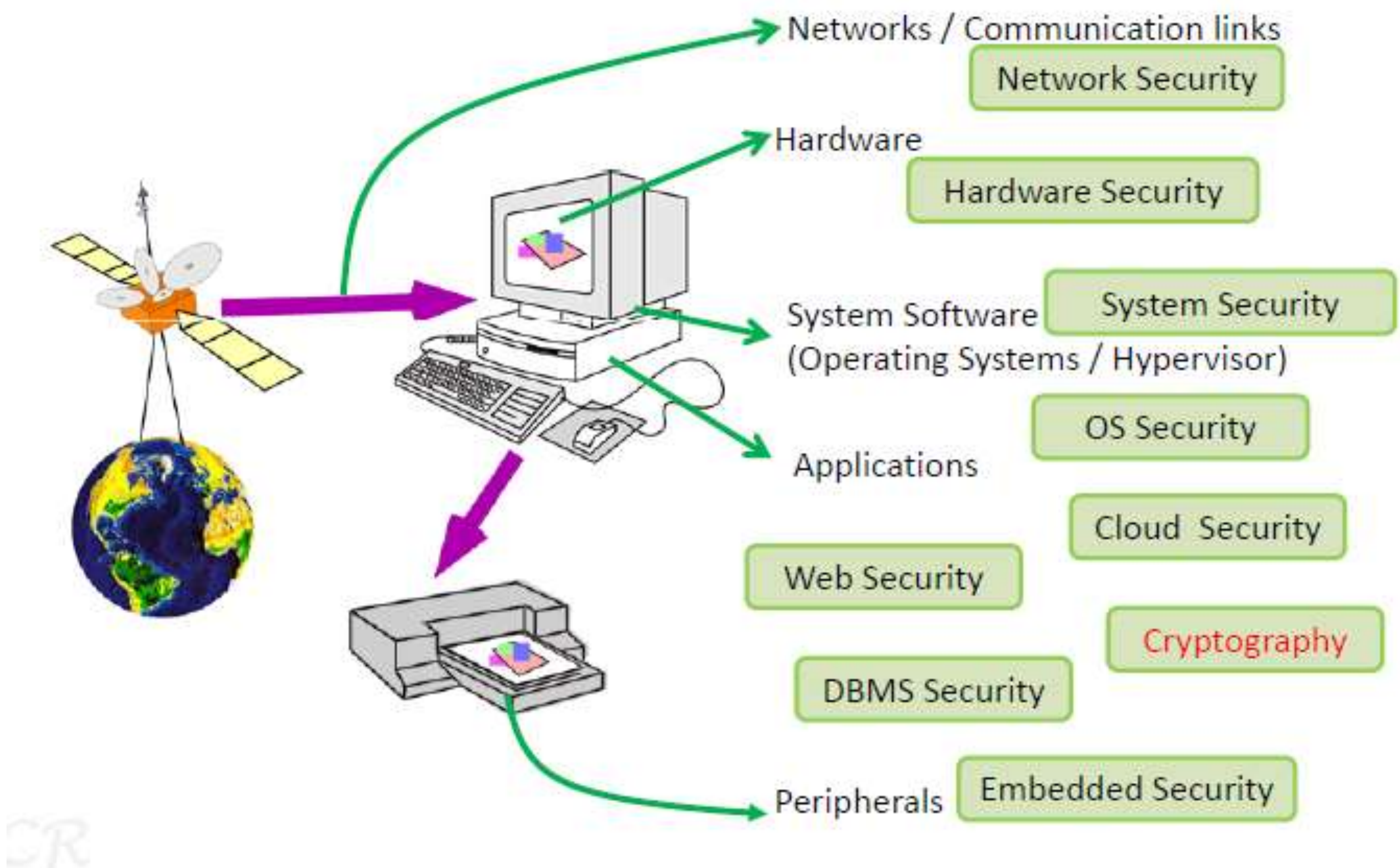
Integrity: The assurance that data received are exactly as sent by an authorized entity (i.e., contains no modification, insertion, deletion or replay).

A loss of integrity is the unauthorized modification or destruction of information.

Availability: Ensuring timely and reliable access to and use of information.

A loss of availability is the disruption of access to or use of information or an information system.

Security Studies (Research) (an ocean)



- Computer Security - generic name for the collection of tools designed to protect data and to stop hackers.
- **Network Security** - measures to protect data during their transmission.
- Internet Security - measures to protect data during their transmission over a collection of interconnected networks.
- Information Security- protect sensitive information from unauthorized access.

Other Definitions of Network Security

- is any protection of access, misuse, and hacking of files and directories in a computer network system.

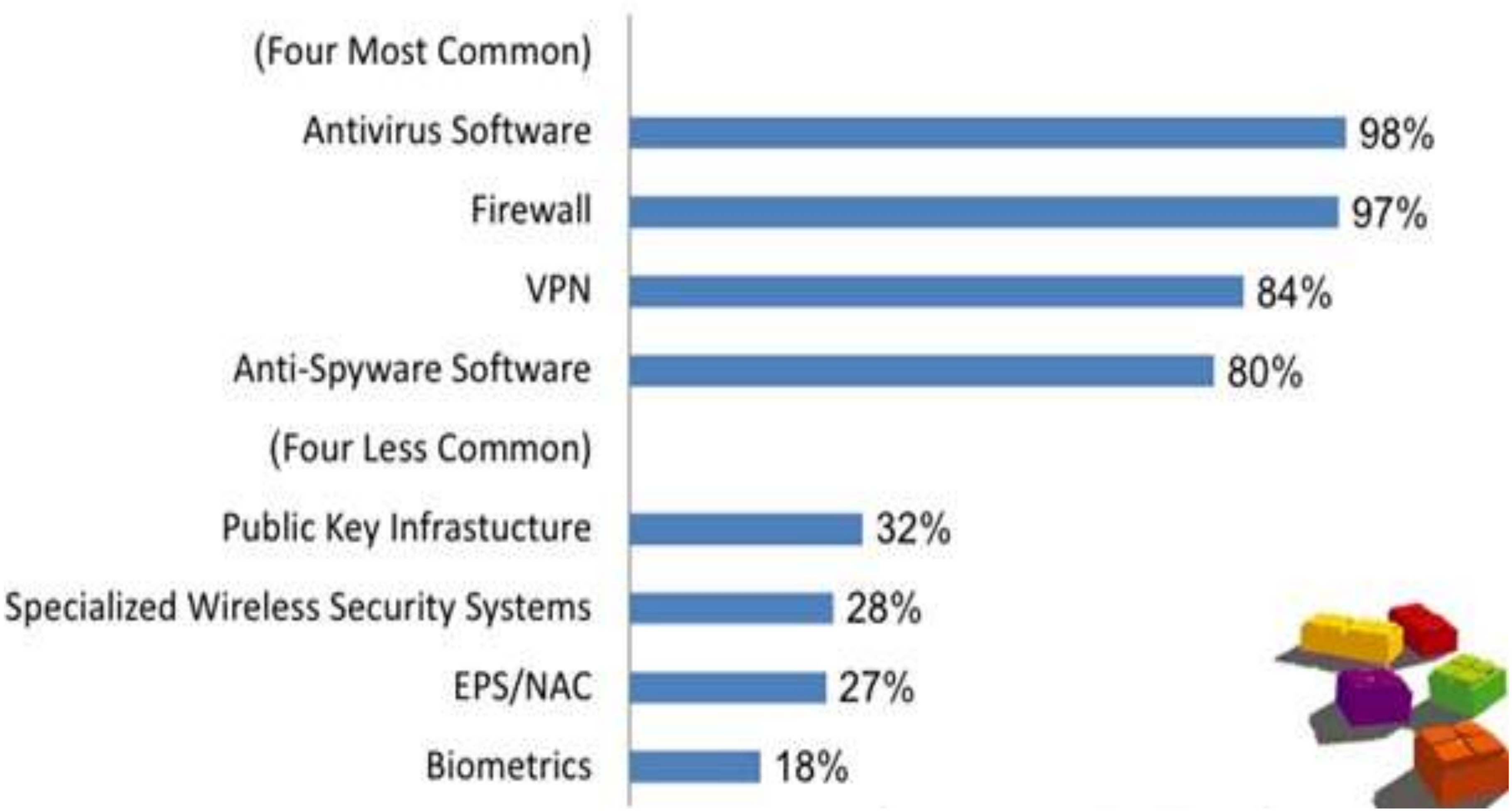
- is a branch of computer science that involves in securing a computer network and network infrastructure devices, to prevent unauthorized access, data theft, network misuse, and data modification.

- In its simplest term, it is a **set of rules and configurations designed to protect the integrity, confidentiality and accessibility of computer networks and data using** both software and hardware technologies.

Threats to Networks

- Virus- is a type of malicious software(malware).
- Worms- replicates while moving across computers.
- Spyware - capture passwords, banking credentials and credit card details.
- Adware- from your hard drive, the Web sites you visit. But it is supported by advertisements.

World Security Technologies used



- Complexity of the system and n/w ↑
- Vulnerabilities ↑
- Task of securing the N/w becomes complex.

Top business organizations spend millions of dollars every year to protect N/W and keep their data safe.

❖ This makes N/W security is an essential part of today's businesses.

- What is cryptography and network security?
- Cryptography is **the study of secure communications techniques that allow** only the sender and intended recipient of a message to view its contents.
- When transmitting electronic data over the network(NS- measures to protect data during their transmission), the most common use of cryptography is to encrypt and decrypt the data.
- The cryptography technique consists of encryption and decryption algorithms.
- Cryptography is an automated mathematical tool that plays a vital role in network security. Cryptography ensures Confidentiality, Authentication and Integrity of a message being communicated.
- It is required to understand the mathematical background of various cryptographic techniques.
- we will also learn some basics of Number Theory.

Number Theory:

Understand the concept of divisibility and the division algorithm.

Understand how to use the Euclidean algorithm to find the greatest common divisor.

Present an overview of the concepts of modular arithmetic.

Discuss key concepts relating to prime numbers.

Understand Fermat’s and Euler’s theorem.

Understand theorem.

Make a presentation on the topic of testing for primality.

Divisibility

We say that a nonzero b **divides** a **if a = mb for some m, where a, b, and m are** integers.

That is, b divides a if there is no remainder on division.

The notation b|a is commonly used to mean b divides a.

Also, if b|a, we say that b is a **divisor of a.**

Properties of Divisibility

- If $a|1$, then $a = \pm 1$.
- If $a|b$ and $b|a$, then $a = \pm b$.
- If $a \mid b$ and $b \mid c$, then $a \mid c$
  - e.g. $11 \mid 66$ and $66 \mid 198$ so $11 \mid 198$
- If $b|g$ and $b|h$, then $b|(mg + nh)$

  for arbitrary integers m and n

- If $b|g$,then g is of the form $g=b \times g1$ for some integers g1.
- If $b|h$, then h is of the form $h=b \times h1$ for some integers h1.
- So $mg+nh=mbg1+nbh1=b \times (mg1+nh1)$
- Here b divides mg+nh

e.g. $b = 7; g = 14; h = 63; m = 3; n = 2$

$7|14$ and $7|63$

To show $7|(3 \times 14 +2 \times 63)$,

we have$(3 \times 14+ 2 \times 63)=7(3 \times 2 + 2 \times 9)$ and

it is obvious that $7|(7(3 \times 2 + 2 \times 9))$.

hence $7 \mid 42+126 = 7|168$

The Division Algorithm

- Given any positive integer n and any nonnegative integer a, if we divide a by n,
- we get an integer quotient q and an integer remainder r that obey the following relationship:

  $a = qn + r$ where $0 <= r < n$; $q =$ ***floor***(a/n)
- The above equation is referred to as the division algorithm.
- **Example: 70 = (4 × 15) + 10**

Symbols for floor and ceiling

- the **floor** and **ceiling** functions gives us the nearest integer up or down.
- The symbols for floor and ceiling are like the square brackets [ ] with the top or bottom part missing:
- But I prefer to use the word form: **floor**(x) and **ceil**(x)

$\lfloor x \rfloor$

floor(x)

$\lceil x \rceil$

ceil(x)

x	Floor	Ceiling	Fractional part
2	2	2	0
2.4	2	3	0.4
2.9	2	3	0.9
−1.1	−2	−1	0.9
−2.7	−3	−2	0.3
−2	−2	−2	0

The Euclidean Algorithm

- One of the basic techniques of number theory is the Euclidean algorithm, which is a simple procedure for determining the Greatest Common Divisor(GCD) of two positive integers.
- notation gcd(a, b) to mean the **greatest common divisor of a and b.**
- gcd(a, b) **is the largest** integer that divides both a and b.

- <u>simple definition</u>: Two integers are **relatively prime** if and only if their only common positive integer factor is 1.

- This is equivalent to saying that *a and b are* relatively prime if gcd(*a, b) = 1.*
  - eg GCD(8,15) = 1
  - hence 8 & 15 are relatively prime
  - Factors of 8 are 1,2,4,8
  - Factors of 15 are 1,3,5,15

no common factors (except 1) define such numbers as **relatively prime**

Finding the Greatest Common Divisor

- Algorithm for easily finding the GCD of two integers.
- Euclidean algorithm has broad significance in cryptography.

Algorithm can be broken down into the following points:

1. Suppose we wish to determine the greatest common divisor *d of the integers a and b; that is determine d = gcd(a, b).*
2. Dividing *a by b and applying the division algorithm, we can state:*

$$a = q_1 b + r_1 \qquad 0 <= r_1 < b$$

3. First consider the case in which *r1 = 0. Therefore b divides a and clearly no* larger number divides both *b and a, because that number would be larger* than *b.*

So we have d = gcd(a, b) = b.

4. The other possibility is *r1 ≠ 0. For this case, we can state* that *d|r1. This is due to the basic properties of divisibility: the relations d|a* and *d|b together imply that d|(a - q1b), which is the same as d |r1.*

Greatest Common Divisor (GCD)

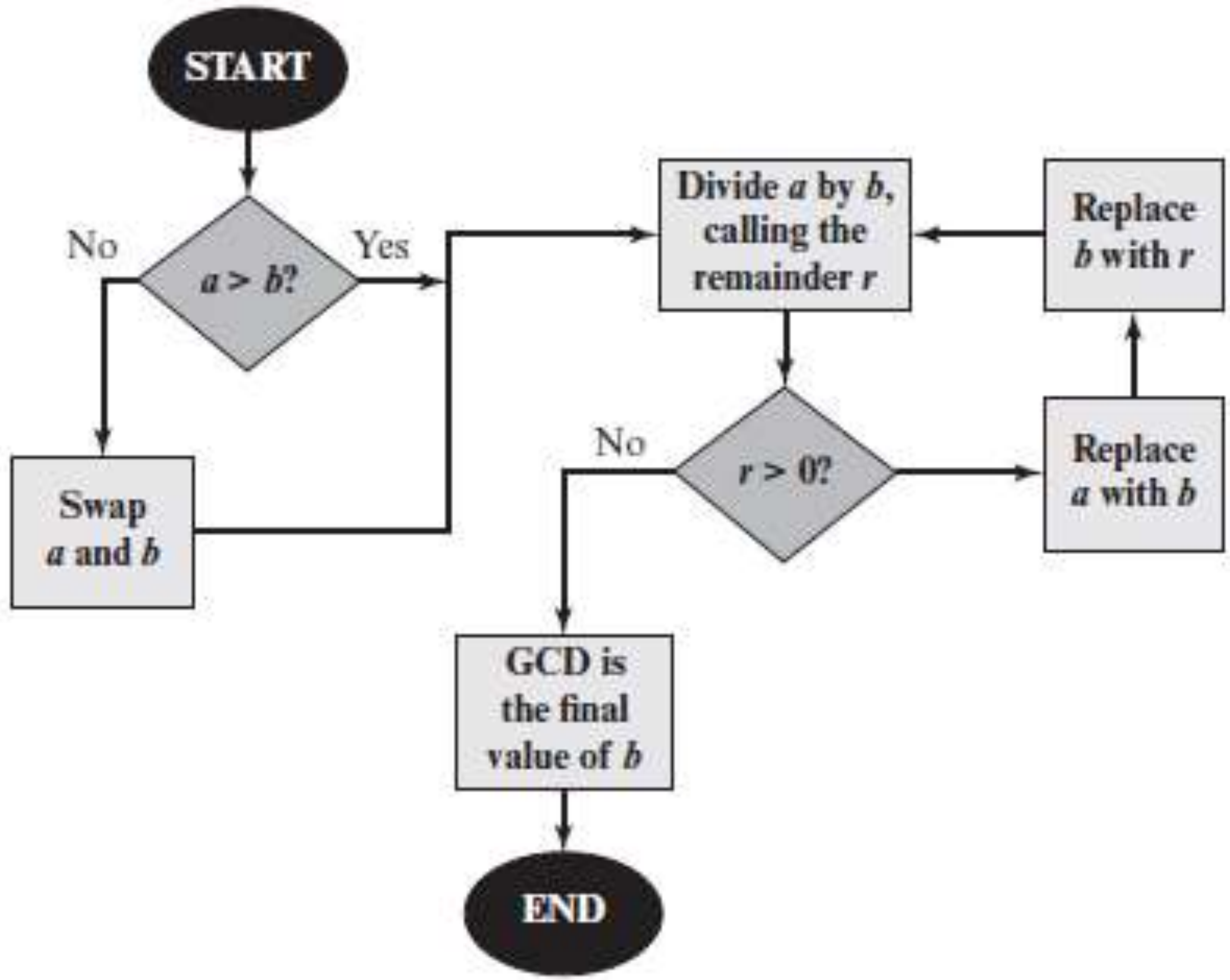
- E.g gcd(10,25)=5 and $GCD(60,24) = 12$

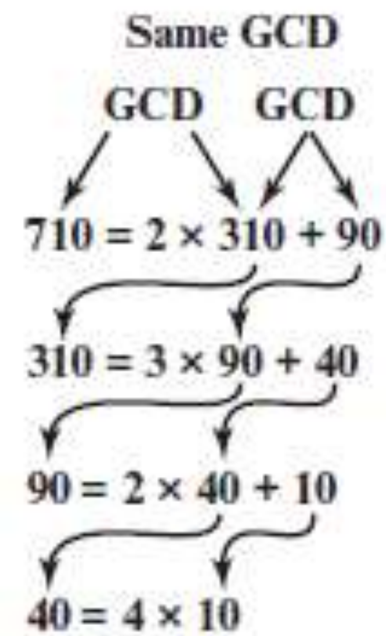
Example: gcd(10,25)=5 using long division

```
10) 25 (2
     20
    -----
       5)10 (2
          10
         -----
      00
```

Test: What is GCD of 12 and 105?

Euclidean Algorithm





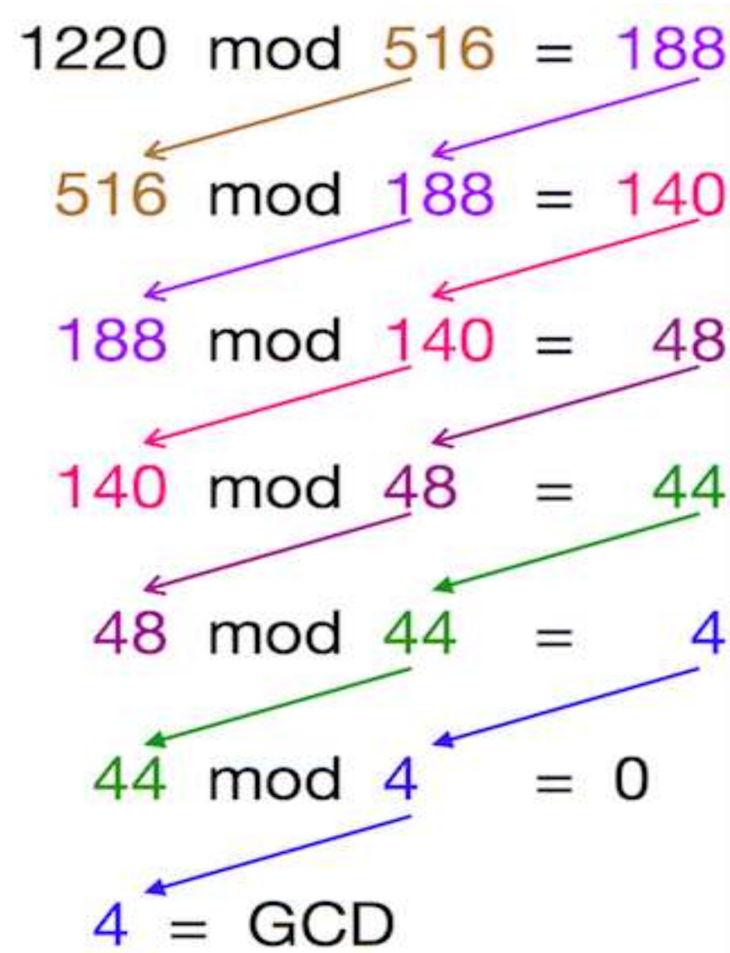
Example:Gcd(710,310)

The result is the following system of equations:

$$
\begin{array}{ll}
a = q_1 b + r_1 & 0 < r_1 < b \\
b = q_2 r_1 + r_2 & 0 < r_2 < r_1 \\
r_1 = q_3 r_2 + r_3 & 0 < r_3 < r_2 \\
\quad\vdots & \quad\vdots \\
r_{n-2} = q_n r_{n-1} + r_n & 0 < r_n < r_{n-1} \\
r_{n-1} = q_{n+1} r_n + 0 & \\
d = \gcd(a, b) = r_n &
\end{array}
$$

Euclidean Algorithm for Greatest Common Divisor (GCD)

- The Euclidean Algorithm finds the GCD of 2 numbers.
- You will better understand this Algorithm by seeing it in action. Assuming you want to calculate the GCD of 1220 and 516, lets apply the Euclidean Algorithm-



Pseudo Code of the Algorithm-

Step 1: **Let a, b be the two numbers**
Step 2: **a mod b = R**
Step 3: **Let a = b and b = R**
Step 4: **Repeat Steps 2 and 3 until a mod b is greater than 0**
Step 5: **GCD = b**
Step 6: Finish

Example with relatively large numbers to see the power of this algorithm:

To find $d = \gcd(a, b) = \gcd(1160718174, 316258250)$		
$a = q_1 b + r_1$	$1160718174 = 3 \times 316258250 + 211943424$	$d = \gcd(316258250, 211943424)$
$b = q_2 r_1 + r_2$	$316258250 = 1 \times 211943424 + 104314826$	$d = \gcd(211943424, 104314826)$
$r_1 = q_3 r_2 + r_3$	$211943424 = 2 \times 104314826 + 3313772$	$d = \gcd(104314826, 3313772)$
$r_2 = q_4 r_3 + r_4$	$104314826 = 31 \times 3313772 + 1587894$	$d = \gcd(3313772, 1587894)$
$r_3 = q_5 r_4 + r_5$	$3313772 = 2 \times 1587894 + 137984$	$d = \gcd(1587894, 137984)$
$r_4 = q_6 r_5 + r_6$	$1587894 = 11 \times 137984 + 70070$	$d = \gcd(137984, 70070)$
$r_5 = q_7 r_6 + r_7$	$137984 = 1 \times 70070 + 67914$	$d = \gcd(70070, 67914)$
$r_6 = q_8 r_7 + r_8$	$70070 = 1 \times 67914 + 2156$	$d = \gcd(67914, 2156)$
$r_7 = q_9 r_8 + r_9$	$67914 = 31 \times 2156 + 1078$	$d = \gcd(2156, 1078)$
$r_8 = q_{10} r_9 + r_{10}$	$2156 = 2 \times 1078 + 0$	$d = \gcd(1078, 0) = 1078$
Therefore, $d = \gcd(1160718174, 316258250) = 1078$		

Euclidean Algorithm Example

Dividend	Divisor	Quotient	Remainder
$a = 1160718174$	$b = 316258250$	$q_1 = 3$	$r_1 = 211943424$
$b = 316258250$	$r_1 = 211943434$	$q_2 = 1$	$r_2 = 104314826$
$r_1 = 211943424$	$r_2 = 104314826$	$q_3 = 2$	$r_3 = 3313772$
$r_2 = 104314826$	$r_3 = 3313772$	$q_4 = 31$	$r_4 = 1587894$
$r_3 = 3313772$	$r_4 = 1587894$	$q_5 = 2$	$r_5 = 137984$
$r_4 = 1587894$	$r_5 = 137984$	$q_6 = 11$	$r_6 = 70070$
$r_5 = 137984$	$r_6 = 70070$	$q_7 = 1$	$r_7 = 67914$
$r_6 = 70070$	$r_7 = 67914$	$q_8 = 1$	$r_8 = 2156$
$r_7 = 67914$	$r_8 = 2156$	$q_9 = 31$	$r_9 = 1078$
$r_8 = 2156$	$r_9 = 1078$	$q_{10} = 2$	$r_{10} = 0$

GCD(1160718174, 316258250)

- This example shows how to find *d = gcd(a, b) = gcd(1160718174, 316258250)*, shown in tabular form.

Dividend	Divisor	Quotient	Remainder
a = 1160718174	b = 316258250	q1 = 3	r1 = 211943424
b = 316258250	r1 = 211943424	q2 = 1	r2 = 104314826
r1 = 211943424	r2 = 104314826	q3 = 2	r3 = 3313772
r2 = 104314826	r3 = 3313772	q4 = 31	r4 = 1587894
r3 = 3313772	r4 = 1587894	q5 = 2	r5 = 137984
r4 = 1587894	r5 = 137984	q6 = 11	r6 = 70070
r5 = 137984	r6 = 70070	q7 = 1	r7 = 67914
r6 = 70070	r7 = 67914	q8 = 1	r8 = 2156
r7 = 67914	r8 = 2156	q9 = 31	r9 = 1078
r8 = 2156	r9 = 1078	q10 = 2	r10 = 0

Example GCD(1970,1066)

Illustrate how we can compute successive instances of GCD(a,b) = GCD(b,a mod b).

Note this MUST always terminate since will eventually get a mod b = 0 (ie no remainder left).

Answer is then the last non-zero value. In this case GCD(1970,1066)=2.

1970 = 1 x 1066 + 904	gcd(1066, 904)
1066 = 1 x 904 + 162	gcd(904, 162)
904 = 5 x 162 + 94	gcd(162, 94)
162 = 1 x 94 + 68	gcd(94, 68)
94 = 1 x 68 + 26	gcd(68, 26)
68 = 2 x 26 + 16	gcd(26, 16)
26 = 1 x 16 + 10	gcd(16, 10)
16 = 1 x 10 + 6	gcd(10, 6)
10 = 1 x 6 + 4	gcd(6, 4)
6 = 1 x 4 + 2	gcd(4, 2)
4 = 2 x 2 + 0	gcd(2, 0)

GCD(18,300)

- conversely can determine the greatest common divisor by comparing their prime factorizations and using least powers.
- eg. $300=2^2 x 3^1 x 5^2$
- $18=2^1 x 3^2$
- Hence $GCD(18,300)=2^1 x 3^1=6$

➢ Euclidean Algorithm to compute GCD(a,b) is:

```
Euclid(a,b)
  if (b=0) then return a;
  else return Euclid(b, a mod b);
```

Find GCD

- 465,527
- 1970,1066
- 24140,16762
- 4655,12075
- 46189,1066
- 1197,5320
- 4389,133
- 2106,2784

The extended Euclidean algorithm

- The extended Euclidean algorithm is particularly useful when a and b are coprime. With that provision, x is the modular multiplicative inverse of a modulo b, and y is the modular multiplicative inverse of b modulo a. Similarly, the polynomial extended Euclidean algorithm allows one to compute the multiplicative inverse in algebraic field extensions and, in particular in finite fields of non prime order. It follows that both extended Euclidean algorithms are widely used in cryptography. In particular, the computation of the modular multiplicative inverse is an essential step in the derivation of key-pairs in the RSA public-key encryption method

Example on Extended Euclidean Algorithm

Find inverse of ‘ a ’ in GCD (a,n) such that $a * a^{-1} = 1 \bmod n$

Find inverse for 9 in gcd(9,26)

q	n	A (inverse value)	R	t1	t2	T3(t1-(t2)*(q)
2	26	9	8	0	1	-2
1	9	8	1	1	-2	3
8	8	1	0	-2	3	-26
	1	0(stop)		3 (answer)	-26	

Here in last step , IF n=1 and b=0 , then inverse exists and its value is t1 value (3). 9*3 = 1 mod 26 . So ‘9’ inverse is ‘3’.

Example on Extended Euclidean Algorithm

Find inverse for 441 in gcd(441,26)

q	n	A (inverse value)	R	t1	t2	T3(t1-(t2)*(q)
0	26	441	26	0	1	0
16	441	26	25	1	0	1
1	26	25	1	0	1	-1
25	25	1	0	1	-1	26
	1	0(stop)		-1(answer)	26	

Here in last step , IF n=1 and b=0 , then inverse exists and its value is t1 value (-1). Convert -1 into positive value i.e. 26-(1mod26) =25 , so 25 is the inverse , 441 * 25 =1 mod 26.

Thank you