WHAT IS RSA ALGORITHM?

- RSA is an asymmetric cryptography algorithm which works on two keys:
  - Public key
  - Private key

3 major steps:

- Key generation
- Encryption
- Decryption

Step:1

- Key generation:
  - Generate 2 prime numbers p & q.
  - Let n=pq.
  - Let m= phi(n)=(p-1)(q-1).
  - Choose a small no e.apply GCD.
  - Find d.mod phi(n)=1.

Step:2

- Encryption
  - Cipher=(message)e mod n.

For encryption, c = me mod n, where m = original message.

Step:3

- Decryption:
  - Message=(cipher)d mod n

For decryption, m = c d mod n, where c is ciphertext.

C++ program to implement RSA algorithm... ..

```
#include<iostream
#include<math.h>
using namespace std;
// find gcd
int gcd(int a, int b)
```

```
    int t;
    while(1)
{
        t= a% b;
```

Continue... .

```
 b= t;
}
}
int main() {
  //2 random prime numbers
  double p = 13;
  double q = 11;
  double n=p*q; //calculate n
  double track;
  double phi= (p-1)*(q-1); //calculate phi
```

Continue... .

```
//public key
//e stands for encrypt
  double e=7;
  //for checking that 1 < e< phi(n) and gcd(e, phi(n)) = 1;  i.e., e and phi(n) are coprime.
  while(e<phi)
{
    track = gcd(e,phi);
    if(track==1)
break;
    else
      e++;
}
```

```
//public key
//e stands for encrypt
  double e=7;
  //for checking that 1 < e< phi(n) and gcd(e, phi(n)) = 1;  i.e., e and phi(n) are coprime.
  while(e<phi)
{
    track = gcd(e,phi);
    if(track==1)
break;
    else
      e++;
 }
```

Continue...

```
//private key
 //d stands for decrypt
 //choosing d such that it satisfies d*e = 1 mod phi
 double d1=1/e;
double d=fmod(d1,phi);
 double message = 9;
 double c = pow(message,e); //encrypt the message
 double m = pow(c,d);
 c=fmod(c,n);
 m=fmod(m,n);
 cout<<"Original Message = "<<message;
```

Continue...

```
    cout<<"\n"<<"p = "<<p;
    cout<<"\n"<<"q = "<<q;
    cout<<"\n"<<"n = pq = "<<n;
    cout<<"\n"<<"phi = "<<phi;
    cout<<"\n"<<"e = "<<e;
    cout<<"\n"<<"d = "<<d;
    cout<<"\n"<<"Encrypted message = "<<c;
    cout<<"\n"<<"Decrypted message = "<<m;
    return 0;
}
```

Output...

```
p=13
q=11
n=pq=143
phi=120
```

Digital Signature Algorithm (DSA)

* A Digital Signature Standard (DSS) is the digital signature algorithm (DSA) developed by the U.S National Security Agency (NSA) in 1991.
* To generate a digital signature for the authentication of electronic documents.
* It is a digital signature Algorithm used for digital signature and its Verification.

Encryption:

* Process of converting electronic data (plain text) into another form called Cipher text. which cannot be easily understood by anyone except the authorized parties.

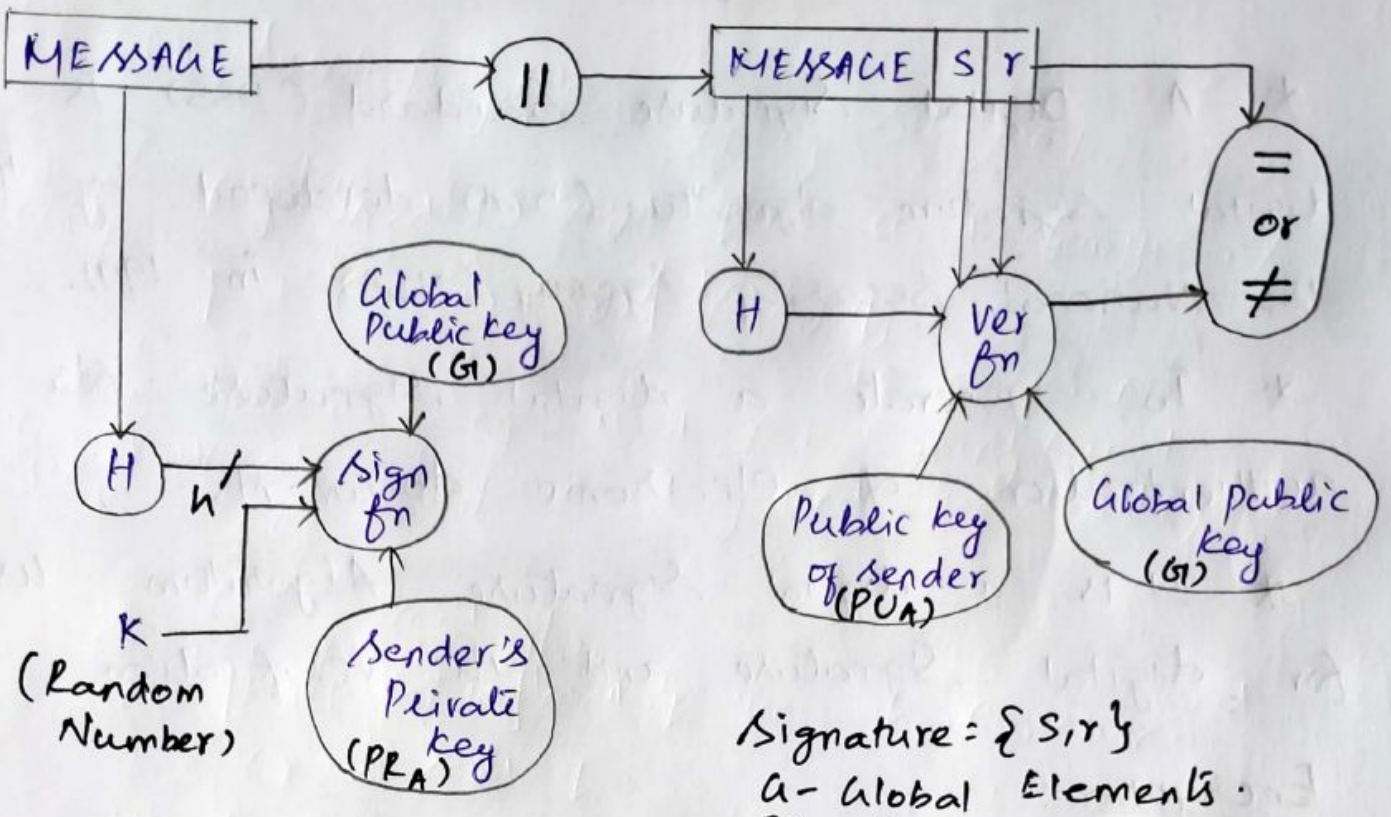
Decryption:

* Process of translating code (Cipher text) to data (plain text).

Digital Signature:

* Encryption is done by using Sender's Private key in this process is automatically known as digital signature.

DIGITAL SIGNATURE ALGORITHM (DSA)



Signature: {S, r}

a - Global Elements.

PR_A - Private key of user A.

PU_A - Public key of user A.

Global public elements:

p: a prime number, a multiple of 64 between 512 and 1024 bits length.

q: a prime divisor of p-1, bit length of 160 bits.

g: $g = h^{(p-1)/q} \bmod p$. $1 < h < p-1$

User's Private key:-

x: random integer where $0 < x < q$

User's Public key:-

y: $g^x \bmod p$

User's Per-Message Secret Number :-

k = random integer where $0 < k < q$

Signing :-

$r = (g^k \bmod p) \bmod q$

$s = [k^{-1}(H(M) + xr)] \bmod q$

Signature = (r, s)

Verifying :-

$w = (s')^{-1} \bmod q$

$a = [H(M') * w] \bmod q$

$b = (r')w \bmod q$

$v = [(g^a y^b) \bmod p] \bmod q$

TEST :

$v = r'$

M = Message to be signed

$H(M)$ = hash of M using SHA-1 [Hash Function]

M', r', s' = received versions of M, r, s.

The following Process explain the entire process in detail:-

* Each Person adopting this scheme has a Public-Private key pair.

* Generally, the key pairs used for encryption/decryption and signing/verifying are different.

* The Private key used for signing is referred to as the signature key and the Public key as the verification key.

* Signer feeds data to the hash function and generates hash of data.

* Hash value and signature key are then fed to the signature algorithm which Produces the digital signature on given hash.

* Signature is appended to the data and then both are sent to the Verifier.

* Verifier feeds the digital signature and the verification key into the verification algorithm.

* The verification algorithm gives some value as Output.

* Verifier also runs same hash function on received data to generate hash value.

* For verification, this hash value and output of verification algorithm are compared.
* Based on the comparison result, verifier decides whether the digital signature is valid.
* Since digital signature is created by 'Private' key of signer and no one else can have this key; the signer cannot repudiate signing the data in future.

Importance of Digital Signature:-

* The most important reason of using hash instead of data directly for signing is Efficiency of the scheme.
* Signing large data through modular exponentiation is computationally expensive and time consuming. [RSA] Hence signing a hash is more efficiency than signing the entire data.

* **Message authentication:** Any process by which a system verifies the identity of a user who wishes to access it.
* **Integrity:-** To ensure that the message was not altered during the transmission.
* **Non-repudiation:-** A way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

DSA Algorithm

V. ARUN
19MCS418

Example:-

Global Public elements: (P, q, g)

P = 7 ✓ # Computed Prime Modulus:

$(P-1) \bmod q = 0$

$(7-1) \% 3 = 0 \Rightarrow 6 \% 3 = 0$ //

q = 3 ✓ # Selected Prime divisor.

g = 4 # $1 < g < P$, $1 < h < P-1$

$g^q \bmod P = 1$ $\quad g = h^{(P-1)/q} \bmod P$

$4^3 \% 7 = 1 \Rightarrow 64 \% 7 = 1$ //

Private key :-

x = 5 # Random (or) Pseudorandom integer

$0 < x < q$ [derived from known starting Point and is typically repeated over and over]

Public key :-

y = 2 # $g^x \bmod P$

$4^5 \% 7 = 1024 \% 7$

$= 2$ //

The Public key: {P, q, g, y} # {7, 3, 4, 2}

The Private key: {P, q, g, x} # {7, 3, 4, 5}

With the Private key {P, q, g, x} = {7, 3, 4, 5},

A Message hash value h = 3 //

h = 3 # The hash value as the Message digest.

k = 2 # Selected: $0 < k < q$

[where k - Per Message Secret Number]

Signing :-

$r=2$ # Computed :

$r = (g^k \bmod p) \bmod q$

$= (4^2 \bmod 7) \bmod 3$

$= (16 \% 7) \% 3$

$= (2 \% 7) \% 3$

$= 2 \% 3$

$= 2$ //

$i=5$ # Computed :

$k * i \bmod q = 1 \Rightarrow 2 * 5 \bmod 3 = 1$ //

$s=2$ # $s = i * (h + r * x) \bmod q$

$\Rightarrow 5 * (3 + 2 * 5) \bmod 3$

$\Rightarrow 5 * (13) \% 3 \Rightarrow 65 \% 3 = 2$ //

Digital Signature = $\{r, s\} = \{2, 2\}$

Verifying :-

$h=3$ # hase value.

$w=5$ # $s * w \bmod q = 1 \Rightarrow (2 * 5) \% 3 = 1$ //

$u_1=0$ # $u_1 = h * w \bmod q \Rightarrow (3 * 5) \% 3 = 0$ //

$u_2=1$ # $u_2 = r * w \bmod q \Rightarrow (2 * 5) \% 3 = 1$ //

$v=2$ # $v = (((g^{u_1}) * (y^{u_2})) \bmod p) \bmod q$

$= (((4)^0 * (2)^1) \% 7) \% 3$

$= ((1 * 2) \% 7) \% 3$

$= (2 \% 7) \% 3 \Rightarrow 2 \% 3 = 2$ //

$v == r$ # Verification Passed.

The Verification value Matches the expected value.

```
1 import java.math.BigInteger;
2 import java.security.*;
3 import java.security.spec.*;
4 import javax.crypto.KeyAgreement;
5
6 public class ECCKeyAgreement
7 {
8 public static void main(String[] args) throws Exception
9 {
10 KeyPairGenerator kpg;
11 kpg = KeyPairGenerator.getInstance("EC","SunEC");
12 ECGenParameterSpec ecsp;
13
14 ecsp = new ECGenParameterSpec("secp192k1");
15 kpg.initialize(ecsp);
16
17 KeyPair kpU = kpg.genKeyPair();
-
18 PrivateKey privKeyU = kpU.getPrivate();
19 PublicKey pubKeyU = kpU.getPublic();
20 System.out.println("User U: " + privKeyU.toString());
21 System.out.println("User U: " + pubKeyU.toString());
22
23 KeyPair kpV = kpg.genKeyPair();
24 PrivateKey privKeyV = kpV.getPrivate();
25 PublicKey pubKeyV = kpV.getPublic();
26 System.out.println("User V: " + privKeyV.toString());
```

```
27 System.out.println("User V: " + pubKeyV.toString());
28
29 KeyAgreement ecdhU =
KeyAgreement.getInstance("ECDH");
30 ecdhU.init(privKeyU);
31 ecdhU.doPhase(pubKeyV,true);
32
33 KeyAgreement ecdhV =
KeyAgreement.getInstance("ECDH");
34 ecdhV.init(privKeyV);
36
37 System.out.println("Secret computed by U: 0x" +
(new BigInteger(1, ecdhU.generateSecret())
38 .toString(16)).toUpperCase());
39 System.out.println("Secret computed by V: 0x" +
(new BigInteger(1, ecdhV.generateSecret())
40 .toString(16)).toUpperCase());
41 }
42 }
```

Conclusion:

uring the past years just have been one of the technologies with a fastest growth.

ince it's version java SE 5. 0 it is possible to use ECC implementation adapted to the JCE\JCA implemented.

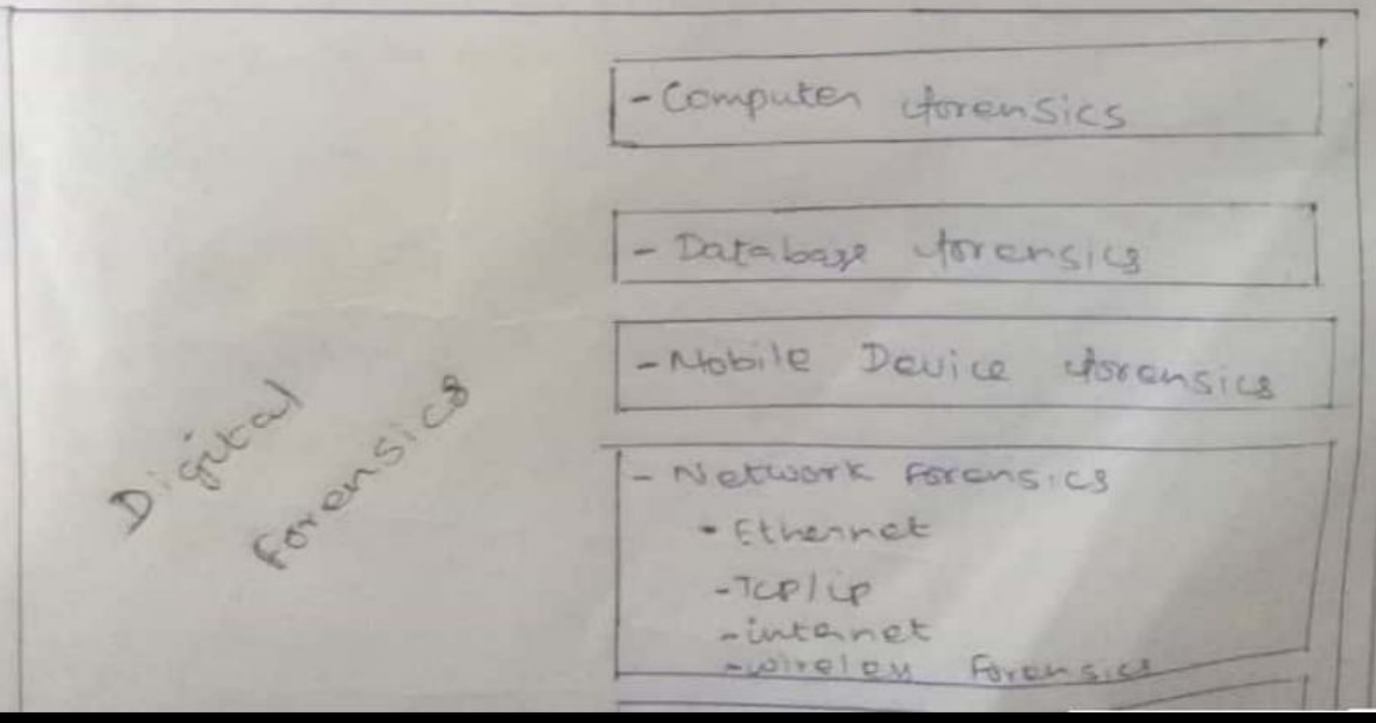
owever scarce there is information about this

CONTENTS

INTRODUTION

• Network Forensics is a categorized as a single branch of digital forensics.

• It includes the areas of a monitering and analyzing computer network monitering traffic and allow individuals together information, compile evidence and/or deduct instrsion



CIA Process for Network Forensic

Capture	Identify	Analyze
Capture packets in Promiscuous mode / SPAN Mirror Ports and Network Taps	Packets are identified and filtered based on specific criteria, such as date and time	Packets are reconstructed and classified based on known and unknown data type, header conflicts etc is performed

Network Forensic Examination Steps

- Identification
- Preservation
- collection
- Examination
- Analysis
- Presentation
- Incident Response

Network Forensic with Network Protocol:

Network forensic method can be applied with in the different network protocol or layers

- ETHERNET
- TCP/IP
- INTERNET
- WIRELESS

Network Forensic Analysis Tools

Function of a network forensic Analysis Tools

- Network tratic capturing and analysis
- Evaluation of network Performence
- Detection Detection of anomalies and misuse of resources
- Determination of network protocol in use.
- Aggregating data from multiple Sources
- Security investigations and incident response
- Production of intellectual Property

Network forensic Tools

- dumpcap, pcapdump and netsniff-ng - Packet Sniffers

- tcpdump, wireshark / tshark and tstat - Protocol Analyzers.

Advantages of Network forensic

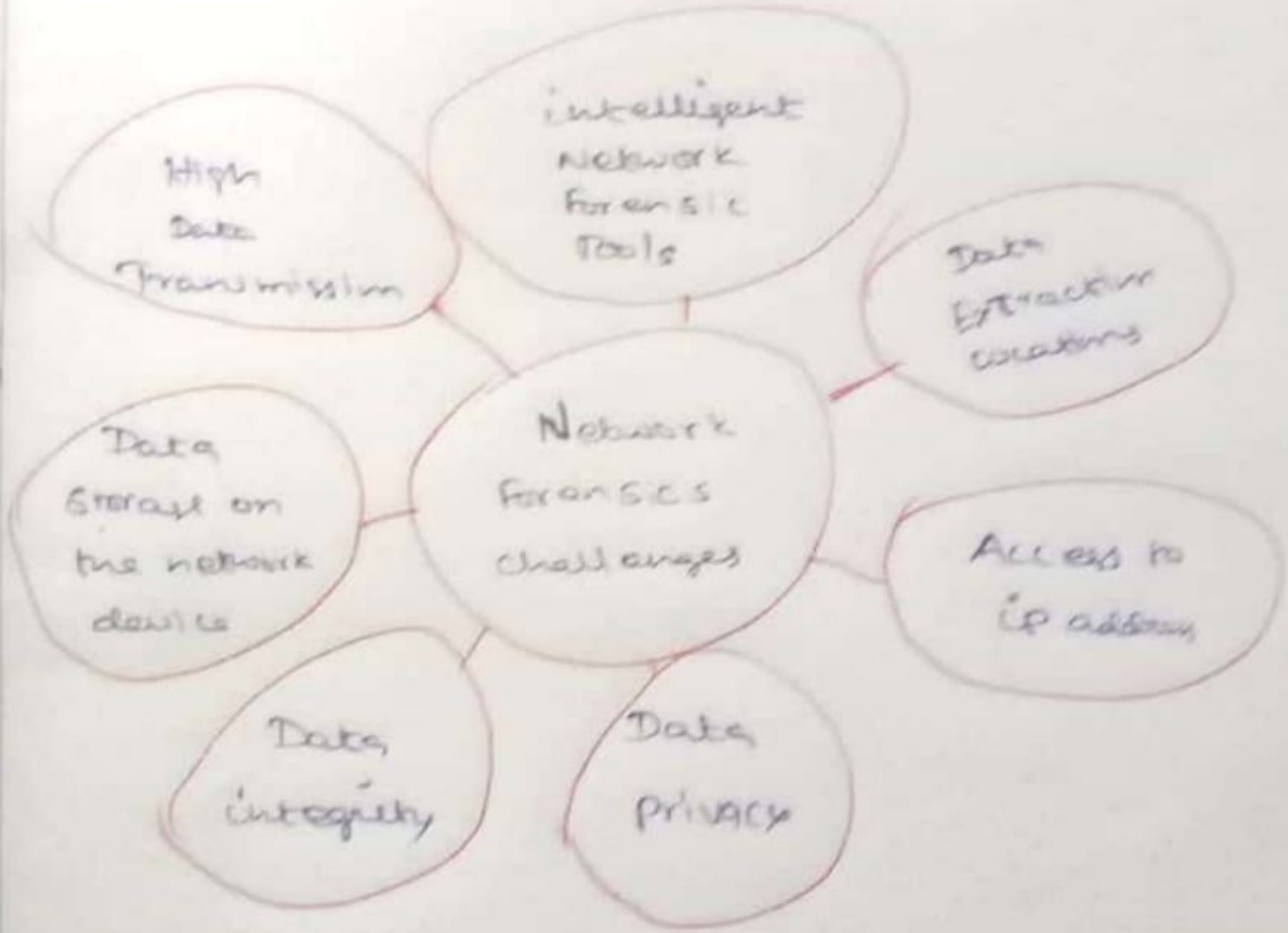
Network Performance Benchmarking

Network Troubleshooting

Transactional Analysis

Security Attack Analysis

Network Forensics Challenges



System Audit

It is an investigation to review the performance of an operational system. The objectives of conducting a system audit are as follows −

- To compare actual and planned performance.
- To verify that the stated objectives of system are still valid in current environment.
- To evaluate the achievement of stated objectives.
- To ensure the reliability of computer based financial and other information.
- To ensure all records included while processing.
- To ensure protection from frauds.

Audit of Computer System Usage

Data processing auditors audits the usage of computer system in order to control it. The auditor need control data which is obtained by computer system itself.

The System Auditor

The role of auditor begins at the initial stage of system development so that resulting system is secure. It describes an idea of utilization of system that can be recorded which helps in load planning and deciding on hardware and software specifications. It gives an indication of wise use of the computer system and possible misuse of the system.

Audit Trial

An audit trial or audit log is a security record which is comprised of who has accessed a computer system and what operations are performed during a given period of time. Audit trials are used to do detailed tracing of how data on the system has changed.

It provides documentary evidence of various control techniques that a transaction is subject to during its processing. Audit trials do not exist independently. They are carried out as a part of accounting for recovering lost transactions.

Audit Methods

Auditing can be done in two different ways −

Auditing around the Computer

- Take sample inputs and manually apply processing rules.
- Compare outputs with computer outputs.

Auditing through the Computer

- Establish audit trial which allows examining selected intermediate results.
- Control totals provide intermediate checks.

Audit Considerations

Audit considerations examine the results of the analysis by using both the narratives and models to identify the problems caused due to misplaced functions, split processes or functions, broken data flows, missing data, redundant or incomplete processing, and nonaddressed automation opportunities.

The activities under this phase are as follows –

- Identification of the current environment problems
- Identification of problem causes
- Identification of alternative solutions
- Evaluation and feasibility analysis of each solution
- Selection and recommendation of most practical and appropriate solution
- Project cost estimation and cost benefit analysis

Security

System security refers to protecting the system from theft, unauthorized access and modifications, and accidental or unintentional damage. In computerized systems, security involves protecting all the parts of computer system which includes data, software, and hardware. Systems security includes system privacy and system integrity.

- System privacy deals with protecting individuals systems from being accessed and used without the permission/knowledge of the concerned individuals.
- System integrity is concerned with the quality and reliability of raw as well as processed data in the system.

Control Measures

There are variety of control measures which can be broadly classified as follows –

Backup

- Regular backup of databases daily/weekly depending on the time criticality and size.
- Incremental back up at shorter intervals.
- Backup copies kept in safe remote location particularly necessary for disaster recovery.
- Duplicate systems run and all transactions mirrored if it is a very critical system and cannot tolerate any disruption before storing in disk.

Physical Access Control to Facilities

- Physical locks and Biometric authentication. For example, finger print
- ID cards or entry passes being checked by security staff.
- Identification of all persons who read or modify data and logging it in a file.

Using Logical or Software Control

- Password system.
- Encrypting sensitive data/programs.
- Training employees on data care/handling and security.
- Antivirus software and Firewall protection while connected to internet.

Risk Analysis

A risk is the possibility of losing something of value. Risk analysis starts with planning for secure system by identifying the vulnerability of system and impact of this. The plan is then made to manage the risk and cope with disaster. It is done to accesses the probability of possible disaster and their cost.

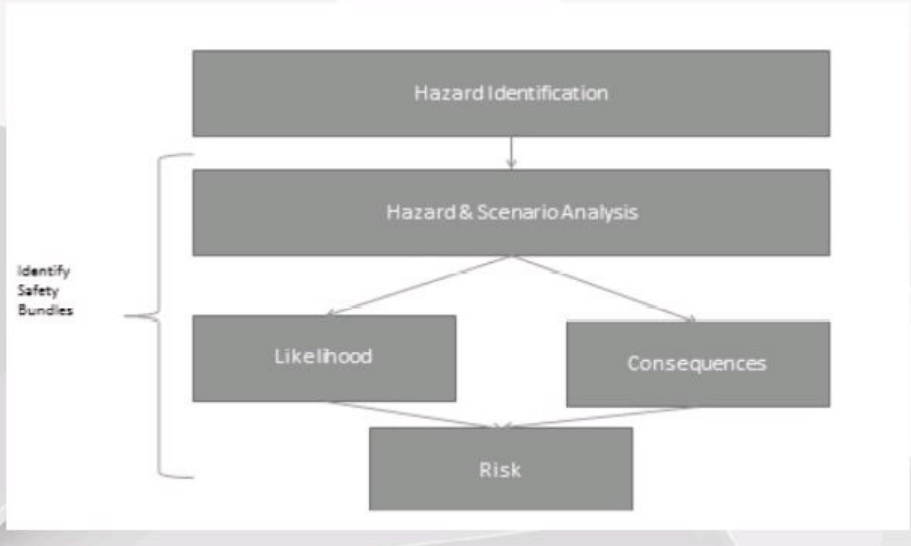
Risk analysis is a teamwork of experts with different backgrounds like chemicals, human error, and process equipment.

The following steps are to be followed while conducting risk analysis –

- Identification of all the components of computer system.
- Identification of all the threats and hazards that each of the components faces.
- Quantify risks i.e. assessment of loss in the case threats become reality.

Risk Analysis – Main Steps

As the risks or threats are changing and the potential loss are also changing, management of risk should be performed on periodic basis by senior managers.



Risk management is a continuous process and it involves the following steps –

- Identification of security measures.
- Calculation of the cost of implementation of security measures.
- Comparison of the cost of security measures with the loss and probability of threats.
- Selection and implementation of security measures.
- Review of the implementation of security measures

Steganography is data hidden within data. Steganography is an encryption technique that can be used along with cryptography as an extra-secure method in which to protect data.

Steganography techniques can be applied to images, a video file or an audio file. Typically, however, steganography is written in characters including hash marking, but its usage within images is also common. At any rate, steganography protects from pirating copyrighted materials as well as aiding in unauthorized viewing.

One use of steganography includes watermarking which hides copyright information within a watermark by overlaying files not easily detected by the naked eye. This prevents fraudulent actions and gives copyrigh protected media extra protection.

There is some concern, sans definite proof, tha the terrorists who plotted and deployed the 9/11 mission in New York City utilized steganography. This is what primarily brought the science of stenography front and center. Data can be stolen and encrypted through a file transfer or, more often than not, through email. And as with what has been suspected for 9/11, steganography can be used for secret communications that deal with terrorist plots.

Why Quantum Cryptography?

- Quantum computing and mathematical advances may
  soon render current cipher algorithms obsolete.

- Classical cryptography techniques allow the key
  transmission to be passively monitored without alerting
  the legitimate users.

Luckily, quantum cryptography addresses both of these issues!

Detecting an Eavesdropper

Heisenberg's uncertainty principle states that there are certain conjugate variables on which limits are placed on the simultaneous knowledge of both. Measuring one variable will necessarily affect the other. Polarization properties of light fall into this category, therefore, an interloper who is trying to intercept and measure the optical signal will invariably affect the system in a such a way that their interference will be noticed.

The Evolution of Q. C.

- In 1970, Stephen J. Weisner designed a theoretical bank note that would be impossible to duplicate, using the laws of quantum mechanics. He proposed using similar principles for cryptography.

- In the 1980's, Charles Bennett and Gilles Brassard used Weisner's ideas to develop the first quantum mechanics based cryptosystem. They were able to transmit, through open air, a distance of about 30 cm by 1989.

- In June of 2003 British Researchers led by Dr. Andrew Shields transmitted a usable key over 100 km of fiber optic cable.

- Nov. 3, 2003 – MagiQ systems announces general availability of world's first commercially available quantum cryptography system, supporting key

- Uses conjugate pairs for information exchange
- Sender retains one particle
- Reciever obtains “matching” particle
- Anything that happens to one particle happens also to its matched particle
- Attempt in intercepting the sent particle results in disturbance of both the sent and retained particle
- Sender is alerted that the message has been compromised
- Inablility to store entangled pairs for more than a

Weaknesses and Limitations of Q.C.

- Only works along unbroken and relatively short fiber optic cables. Record as of March, 2004 is 120 km.
- Doesn’t solve authentication problem.
- Doesn’t address some of the weakest links in data security such as human corruptibility and key storage.

Conclusion

Quantum cryptography developments promise to address some of the problems that plague classical encryption techniques such as the key distribution problem and the predicted breakdown of the public/ private key system. quantum cryptography operates on the Heisenberg uncertainty principle and random polarization of light. Another purely theoretical basis involves EPR entangled pairs.

Due to the high cost of implementation and the adequacy of current cryptological methods, it is unlikely that quantum cryptography will be in widespread use for several years.

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio, video or image data.

It is typically used to identify ownership of the copyright of such signal.

"Watermarking" is the process of hiding digital information in a carrier signal.

Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners.

It is prominently used for tracing copyright infringements and for banknote authentication.

digital watermarks are often only perceptible under certain conditions.

HISTORY

The term "Digital Watermark" was coined by Andrew Tirkel and Charles Osborne in December 1992.

The first successful embedding and extraction of a steganographic spread spectrum watermark was demonstrated in 1993 by Andrew Tirkel, Charles Osborne and Gerard Rankin.

Watermarks are identification marks produced during the paper making process.

1.Copyright protection

2.Source tracking (different recipients get differently watermarked content)

3.Broadcast monitoring (television news often contains watermarked video from international agencies)

4.Video authentication

5.Software crippling on screencasting and video editing software programs, to encourage users to purchase the full version to remove it.

6.ID card security.

7.Fraud and Tamper detection.

8.Content management on social networks.

CLASSIFICATION

Digital watermarking techniques may be classified in several ways.

1.Robustness

2.Perceptibility

3.Capacity

4.Embedding method

REVERSIBLE DATA HIDING

Reversible data hiding is a technique which enables images to be authenticated and then restored to their original form by removing the digital watermark and replacing the image data that had been overwritten.

This would make the images acceptable for legal purposes.

The US Army also is interested in this technique for authentication of reconnaissance images.

WATERMARKING FOR RELATIONAL DATABASE

Digital watermarking for relational databases has emerged as a candidate solution to provide copyright protection, tamper detection, traitor tracing, and maintaining integrity of relational data.

Many watermarking techniques have been proposed in the literature to address these purposes.

DNA CRYPTOGRAPHY CAN BE DEFINED AS A HIDING DATA IN TERMS OF DNA SEQUENCE.

- Adenine (A)
- Thymine (T)
- Cytosine (C)
- Guanine (G)

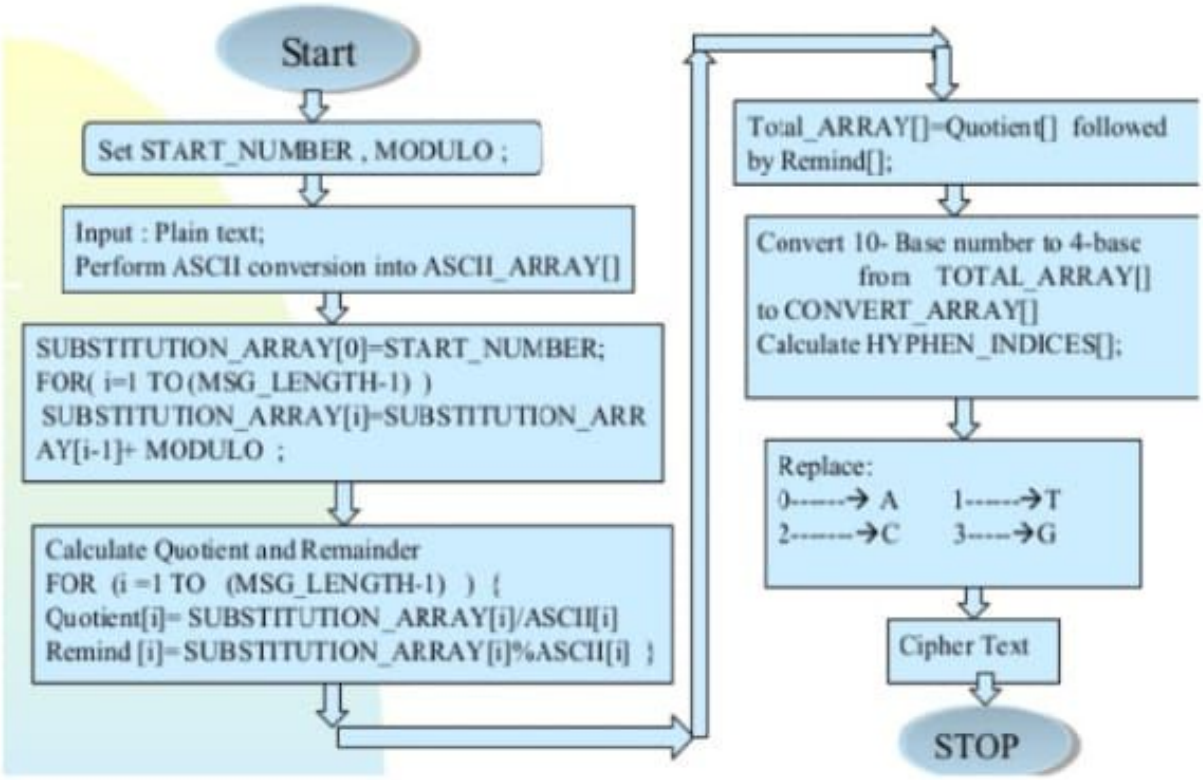
The easiest way to encode is to represent these four units as four figures:

- A(0) - 00 G(3) - 11
- T(1) - 01
- C(2) - 10

DNA ENCRYPTION TECHNIQUE

- key = {Starting _ Number, Modulus, Hyphen _ Indices _ Array[]}
- Starting _ Number: Used to generate some sequential integer.
- Substitution _ Array[i] =Substitution _ Array[i-1] + Modulus;
- Modulus: Difference between each sequential integer in substitution _ Array[]
- Hyphen _ Indices _Array[]: used to separate number from sequence.

ENCRYPTION TECHNIQUE



ENCRYPTION TECHNIQUE

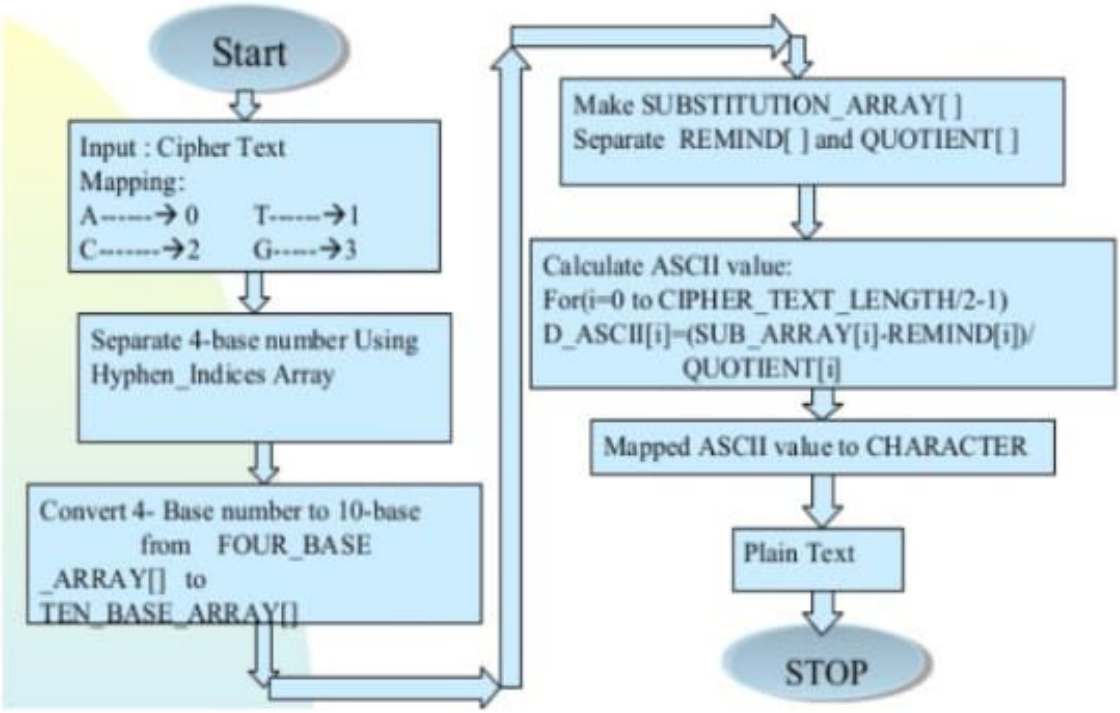
Character	ASCII []	SUBSTITUTION ARRAY []	DIVISION	Quotient[]	Remainder[]
M	77	877	877/77	11	30
E	69	902	902/69	13	5
S	83	927	927/83	11	14
U	85	952	952/85	11	11
K	75	977	977/75	13	2

```
**************************DATA ENCRIPTION**********
ENTER PLAIN TEXT:MESUK

CORRESPONDING ASCII VALUE:77 69 83 85 75
SUB ARRAY:100 125 150 175 200
QUOTIENT:1 1 1 2 2
REMAINDER:23 56 67 5 50
QUOTIENT AND REMAINDER:1 1 1 2 2 23 56 67 5 50
FOur base data:1 1 1 2 2 113 320 1003 11 302
HYPHEN INDICES:2 4 6 8 10 14 18 23 26

CYPHER TEXT:  TTTCCTTGGCATAAGTTGAC
```

DECRYPTION TECHNIQUE



DECRYPTION TECHNIQUE

Cipher Text:TTTCCTTGGCATAAGTTGAC

QUOTIENT	REMAINDER	For(i=0 to cipher_text_length/2) D_ASCII[i]=(SUB_ARRAY[i]-REMIND[i])/ QUOTIENT[i]	Character
11	30	(877-30)/11= 77	M
13	5	(902-5)/13= 69	E
11	14	(927-14)/11= 83	S
11	11	(952-11)/11= 85	U
13	2	(977-2)/13 = 75	K

```
****************DATA DECRYPTION*****************....
CIPHER TEXT:                TTTCCTTGGCATAAGTTGAC
MAPPED SEQUENCE TO NUMBER:11122113320100311302
FOUR BASE QUOTIENT & REMAINDER:1 1 1 2 2 113 320 1003 11 302
TEN BASE QUOTIENT & REMAINDER:1 1 1 2 2 23 56 67 5 50
DECRYPTED QUOTIENT:1 1 1 2 2
DECRYPTEDREMAINDER:23 56 67 5 50
DECRYPTED ASCII VALUE:77 69 83 85 75

DECRYPTED MESSAGE:MESUK
```