CS547 - Foundation of Computer Security
Assignment 4: Understanding Crypto Basics

Prepared by Harsh Kasyap
1921CS01, Ph.D. (CSE), Dept. of CSE, IIT Patna

November 2019

Question 1 (a)
Writes AES (Rindael) algorithm as discussed in class.
Answer
The AES (*Advanced Encryption Standard*) was published by NIST (*National Institute of Standards and Technology*) in 2001. AES is a block cipher intended to replace DES (*which was published in 1977*) for commercial applications. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.

Reasons for Origin of AES
The potential vulnerability of DES to a *brute-force attack*, there has been considerable interest in finding an alternative. One approach is to design a completely new algorithm or another alternative, which would preserve the existing investment in software and equipment, is to use multiple encryption with DES and multiple keys.
Therefore, in 1999, NIST issued a new version of its standard triple DES which in essence involves repeating the DES algorithm three times on the plain-text using two or three different keys to produce the ciphertext. 3DES has two attractions are as follows that assure its widespread use over the next few years:

- With its 168-bit key length, it overcomes the vulnerability to brute-force attack of DES.
- The underlying encryption algorithm in 3DES is the same as in DES.

This algorithm has been subjected to more scrutiny and no effective cryptanalytic attack based on the algorithm rather than brute force has been found. *The principal drawback of 3DES* are as follows,

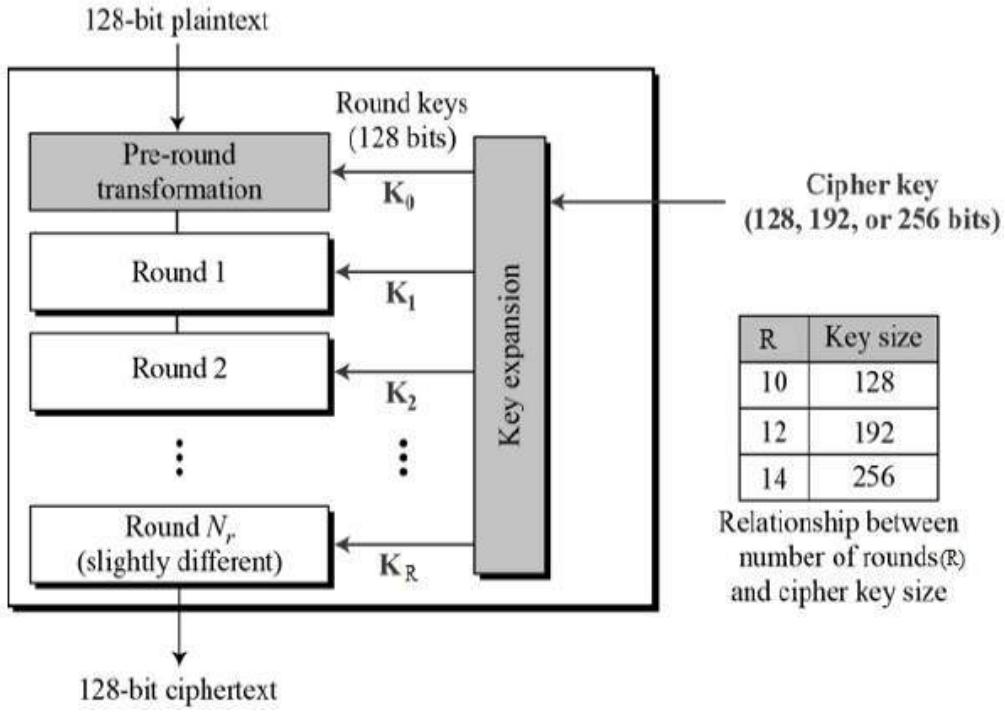
- The algorithm is relatively sluggish in software.
- In original DES, does not produce efficient software code. So, 3DES, which has three times as many rounds as DES, is correspondingly slower.

- Both DES and 3DES use a 64-bit block size.

For reasons of both **efficiency and security**, a larger block size is desirable. Because of these drawbacks, 3DES is not a reasonable candidate for long-term use. Therefore, NIST comes with new algorithm AES.

AES Structure and Algorithm

AES uses a 128-bit block size and a key size of 128, 192, or 256 bits. AES does not use a Feistel structure. Instead, each full round consists of four separate functions: *byte substitution*, *permutation*, *arithmetic operations over a finite field*, and *XOR with a key*. Compared to public-key ciphers such as RSA, the structure of AES and most symmetric ciphers is quite complex and cannot be explained as easily as many other cryptographic algorithms. The schematic of AES structure is shown in below figure 1.



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

Figure 1: AES Structure

- The cipher consists of N rounds, where the number of rounds depends on the key length: 10 rounds for a 16-byte key, 12 rounds for a 24-byte key, and 14 rounds for a 32-byte key.
- There is a initial single transformation (**AddRoundKey**). Here, each byte of the state is combined with a block of the round key using bitwise xor. The first matrix is **State**, and the second matrix is the **round key**. The **inverse add round key transformation** is identical to the forward

add round key transformation, because the XOR operation is its own inverse. The following figure 2 is illustrate the process of AddRoundKey The

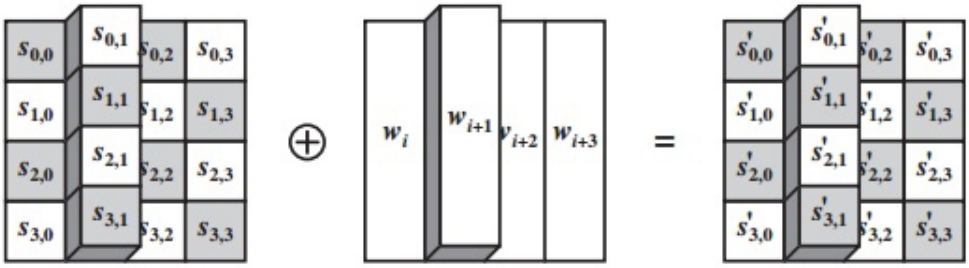


Figure 2: Add Round Key Transformation

example reflects the AddRoundKey process in below figure 3.

47	40	A3	4C
37	D4	70	9F
94	E4	3A	42
ED	A5	A6	BC

⊕

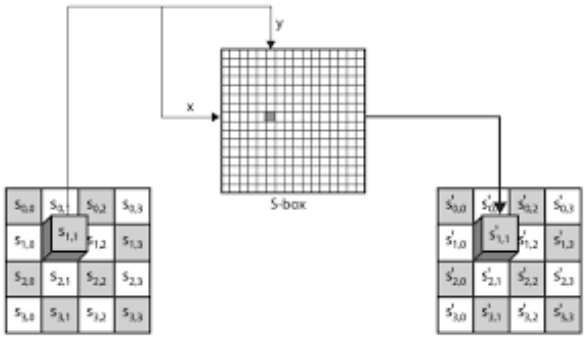
AC	19	28	57
77	FA	D1	5C
66	DC	29	00
F3	21	41	6A

=

EB	59	8B	1B
40	2E	A1	C3
F2	38	13	42
1E	84	E7	D6

Figure 3: Add Round Key Transformation Example

- The first N - 1 rounds consist of four distinct transformation functions:
  - **SubBytes**: Uses an S-box to perform a byte-by-byte substitution of the block. Each individual byte of State is mapped into a new byte in the following way: The leftmost 4 bits of the byte are used as a row value and the rightmost 4 bits are used as a column value. These row and column values serve as indexes into the S-box to select a unique 8-bit output value. The **inverse substitute byte transformation**, called InvSubBytes, makes use of the inverse S-box. Here in figure 4a



(a) Substitute Byte Transformation

EA	04	65	85
83	45	5D	96
5C	33	98	B0
F0	2D	AD	C5

→

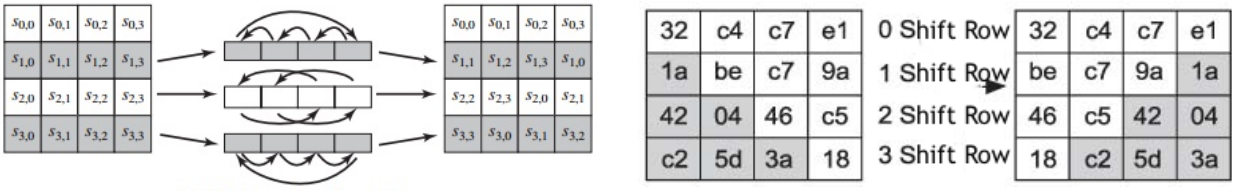
87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

(b) Substitute Byte Transformation Example

Figure 4: Substitute Byte Transformation Process with Example

shows SubBytes transformation process and example in figure 4b.

– **ShiftRows**: a transposition step where the last three rows of the state are shifted cyclically a certain number of steps. The figure 5a



(a) Shift Row Transformation

(b) Shift Row Transformation Example

Figure 5: Shift Row Transformation Process with Example

illustrate the ShiftRow process and example shown in figure 5b. The **inverse shift row transformation**, called InvShiftRows, performs the circular shifts in the opposite direction for each of the last three rows, with a 1-byte circular right shift for the second row, and so on.

– **MixColumns**: a linear mixing operation which operates on the columns of the state, combining the four bytes in each column.The figure 6 illustrate the MixColumn process and example shown in figure 7. Each

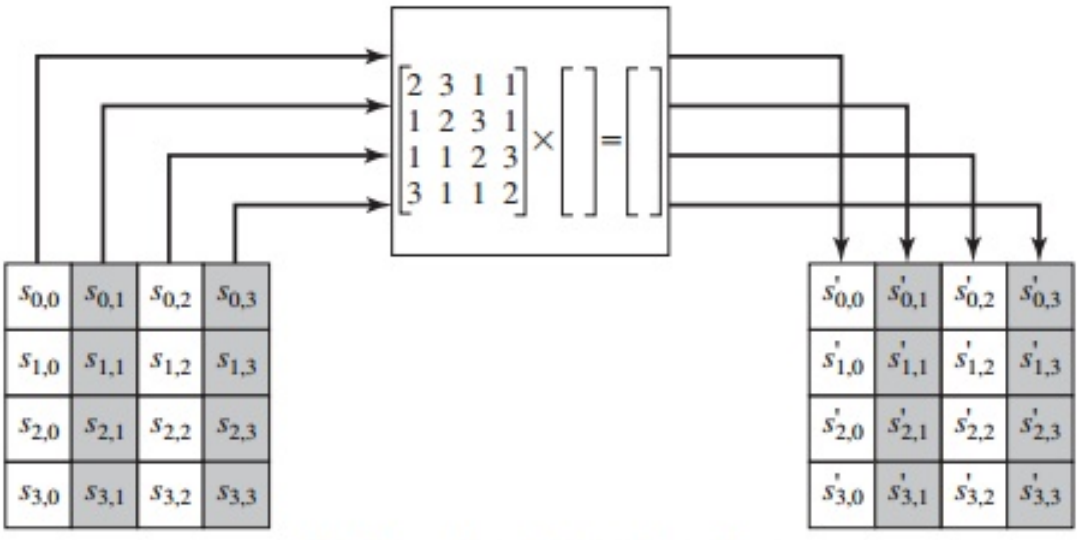


Figure 6: Mix Column Transformation

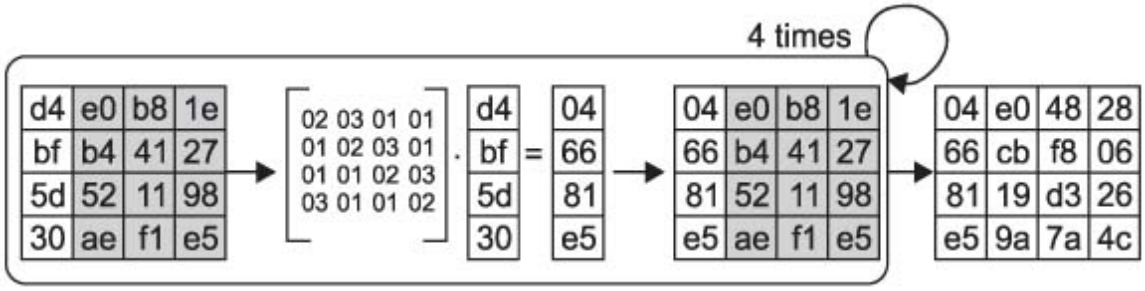


Figure 7: Mix Column Transformation Example

byte of a column is mapped into a new value that is a function of all

four bytes in that column. The transformation can be defined by the above matrix multiplication on State. Each element in the product matrix is the sum of products of elements of one row and one column. The inverse mix column transformation, called InvMixColumns.

  - **AddRoundKey**:A simple bitwise XOR of the current block with a portion of the expanded key. Rest process is same as illustrate in first step.

- The final round contains only three transformations.
  - SubBytes
  - ShiftRows
  - AddRoundKey
- Each transformation takes one or more 4×4 matrices as input and produces a 4×4 matrix as output.
- The key expansion function generates N + 1 round keys, each of which is a distinct 4×4 matrix. Each round key serve as one of the inputs to the AddRoundKey transformation in each round.
- For both encryption and decryption, the cipher begins with an AddRoundKey stage, followed by nine rounds that each includes all four stages, followed by a tenth round of three stages.
- Only the AddRoundKey stage makes use of the key. For this reason, the cipher begins and ends with an AddRoundKey stage.
- Each stage is easily reversible. For the Substitute Byte, ShiftRows, and MixColumns stages, an inverse function is used in the decryption algorithm. For the AddRoundKey stage, the inverse is achieved by XORing the same round key to the block, using the result that $A \oplus B \oplus B = A$.
- As with most block ciphers, the decryption algorithm makes use of the expanded key in reverse order. However, the decryption algorithm is not identical to the encryption algorithm. This is a consequence of the particular structure of AES.
- The final round of both encryption and decryption consists of only three stages. Again, this is a consequence of the particular structure of AES and is required to make the cipher reversible.
- Figure 8 shows AES Encryption and Decryption algorithm process.

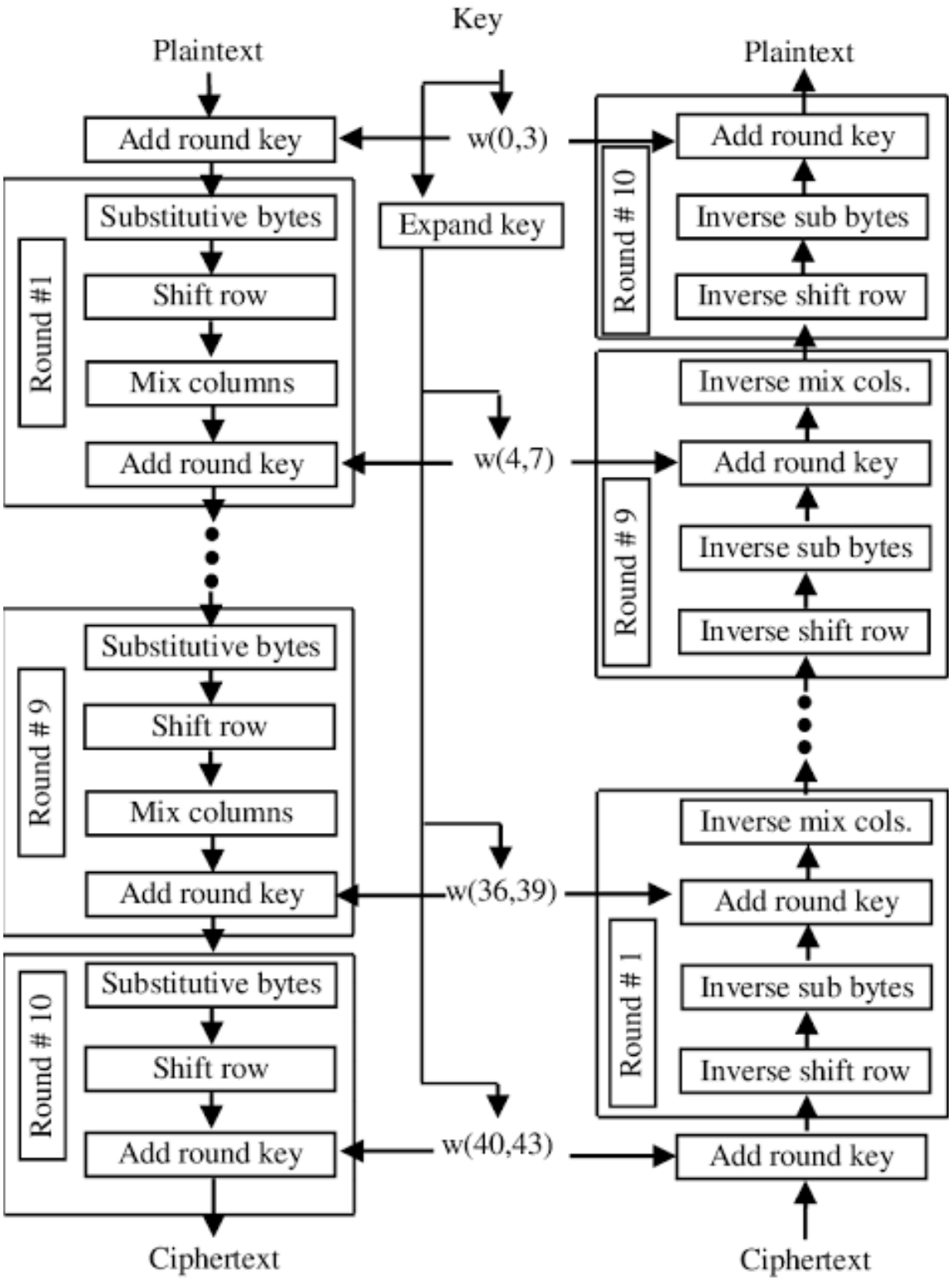


Figure 8: AES Encryption and Decryption

Question 1 (b)
Discuss the diffusion and confusion properties achieved by AES.
Answer
The Advanced Encryption Standard (AES) has both excellent confusion and diffusion. Its confusion look-up tables are very non-linear and good at destroying patterns. Its diffusion stage spreads every part of the input to every part of the output: changing one bit of input changes half the output bits on average. Both confusion and diffusion are repeated multiple times for each input to increase the amount of scrambling. The secret key is mixed in at every stage so that an attacker cannot precalculate what the cipher does.

It can illustrate further as the add key layer ensures the encryption function is only computable by someone who knows the key. Adds some confusion because the key is (psuedo) random. The subBytes s-box layer creates confusion each symbol is mapped to another symbol in a way that impedes common methods of cryptanalysis (high resistance to linear and differential cryptanalysis).

The shiftRows and mixColumns operations combine to provide full diffusion over the course of 2 rounds. The state is a 4×4 grid of 8-bit words. mixColumns operates vertically on each 4 word/32-bit column, One bits difference in any word in the input column will spread to multiple places in multiple words in the output column. shiftRows ensures that over the course of successive rounds different words are grouped up as inputs to the mixColumn function.

None of this would happen if one used a simple one-stage scramble based on a key. Input patterns would flow straight through to the output. It might look random to the eye but analysis would find obvious patterns and the cipher could be broken.

Question 1 (c)
Execute the AES code and discuss the avalanche property exhibited by AES.
Answer
Avalanche Property: A change in one bit of the plaintext or one bit of the key should produce a change in many bits of the ciphertext.

Test Perform: To perform the test we change plaintext bit to "hi" instead of "hy" and "11" instead of "21" and "22" instead of "21" the result obtained is is 80.77%, 91.66% and 92.86% respectively.
Observation: From the below result shown in table 1, It can see that the cipher text is very strong for very simple plaintext.

Table 1: Avalanche Effect in AES: Change in Plaintext

Plain Text	Cipher Text	Avalanche Effect
parthasarathi parthasarathy	b'GLHBF6McZ9Qb72tdWm705A==' b'qoy6PLOPSzcSIPUVBFBK8A=='	77.77% (21/27)*100
abcd1122 abcd2122	b'bG4PF8u2XKAdyuR+lgwqbg==' b'qIWQ26HdLHYSPTp7vQAu2Q=='	81.48% (22/27)*100
abcdefgh11112222 abcdefgh11112221	b'EMeIVUMefqX3Zi/gQTCAjYZQyW7A+Sv4hd4IhYjBTWo=' b'8tBhGWLjRulrkjRKMShBF5duVNDBz8QG+mV2uAoPExM='	91.48% (43/47)*100

Question 2

Let IIT Patna wish to transfer all the files documents digitally. Prepare a case study and summarize through a table highlighting the following.

a) Define the security threats

b) Security Services required to address that threat

c) Cryptographic mechanisms required with proper justification.

Answer

Transfer all the files or documents digitally is a good idea and having lots of benefits, but number of threats attached with it. The most well-known of these risks is *cyberattacks*. It is interesting to note that not all attacks come from the outside. *IBM's 2016 Cyber Security Intelligence Index*[1] discovered that 60% of cybersecurity threats come from people inside the institute or company.
Cyberattacks threaten IIT Patna's data, leaving confidential projects, research and funding documents such as insider information exposed. Finance remains one of the most vulnerable areas. IIT Patna is a public and premier government institute of India, it may face reputational risk also if such security attacks exposes.
Therefore, the focus for IIT Patna's administrator and technology resources must shift from being reactive, and addressing cybersecurity incidents after they occur, to implementing a proactive strategy and framework to identify and cyberthreats before they can harm the institute.

Security Threats

Security threats can be anything like Software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion.

[1]Marc van Zadelhoff, "The Biggest Cybersecurity Threats Are Inside Your Company", Harvard Business Review, September 19, 2016

Software attacks means attacks (basis of infection) by Viruses, Worms, Trojan Horses, bots and attacks (basis of actions) Spyware, Ransomware, Rootkits, Zombies, etc.
The table 2 shows list of security threats and its impacts to IIT Patna data resources.

Table 2: Example of Security Threats to IIT Patna's Document Digitization

Security Threats	**Threat Consequence**	**Security Concern**
Sensitive Data and Intellectual Property	steal and profit from sensitive personal project, research confidential documents and financial information from students, faculty, and staff Black market for privacy data	Confidentiality Integrity
Control Network Infrastructure	Target victims in other industries, on the assumption that their activity will appear less suspicious originating from a reputable institution's network. Malware Attack	Availability
Insider threat or Malicious User or Human Error	Misconfiguration, complacency, lack of awareness, Insiders (curious, careless, or disgruntled employees), Untrained Staff Pose Security Threat Virus Attack	Integrity Availability Confidentiality
Physical threats	Shoulder surfing, Dumpster diving, Evil hardware, Lost or stolen hardware	Physical Infrastructure
Third party APIs	Exposing the institution and its data at risk.	Abstraction
Hacktivists	Cyber-activists who attack for political, egotistical, or philosophical reasons or Anonymous, LulzSec	Availability Confidentiality Integrity
Mobile Devices	Administrators and users take their work on the go, Use untrusted networks, Lost / stolen devices or media	Availability Confidentiality Integrity

Security Services Requirement

- *Security requirements for Database of files/documents*: Physical and Logical Database Integrity, Element Integrity, Audit-ability, Access Control, User Authentication
- *Access Decisions*: Availability of Data, Acceptability of Access, Assurance of Authenticity
- *Network Security Control*: Security Threat Analysis, Encryption, Content Integrity, Strong Authentication, Access Control, Wireless Security, Alarms and Alerts, Traffic Flow Security, Control Review

- *Others*: Firewall, Intrusion Detection Systems, Security of E-mail and its data.

Cryptographic Mechanisms Required

- Secure Data Encryption Algorithm: Encryption plays an important role in securing many different types of information technology (IT) assets. It provides the following:
  - Confidentiality encodes the message's content.
  - Authentication verifies the origin of a message.
  - Integrity proves the contents of a message have not been changed since it was sent.
  - Non-repudiation prevents senders from denying they sent the encrypted message.

  The primary purpose of encryption is to protect the confidentiality of digital data stored on computer systems or transmitted over the internet or any other computer network.
  In addition to security, the adoption of encryption is often driven by the need to meet compliance regulations. A number of organizations and standards bodies either recommend or require sensitive data to be encrypted in order to prevent unauthorized third parties or threat actors from accessing the data. Popular Encryption algorithms are AES, DES, 3DES, RSA, ECC etc.

- Cryptographic Hash Function: Hash functions provide another type of encryption. Hashing is the transformation of a string of characters into a fixed-length value or key that represents the original string. When data is protected by a cryptographic hash function, even the slightest change to the message can be detected because it will make a big change to the resulting hash.Popular hashing algorithms include the Secure Hashing Algorithm (SHA-2 and SHA-3) and Message Digest Algorithm 5 (MD5).

- Digital Signature: It is required for all types of transactions of data or files like pdf or doc files, email data etc. DS satisfy the properties of unforgeable, authentic, not alterable, not reusable. RSA, DSA is considered one of the most preferred digital signature algorithms used today.

- Encrypted Database: Documents or files are must store in encrypted form. So, that only authorized and authenticate person can access it. Different databases, such as SQL, Oracle, Access and DB2, have unique encryption and decryption methods.