



# INTERNATIONAL INSTITUTE OF PROFESSIONAL STUDIES

## III INTERNAL ASSIGNMENT

### TEST - 1

## INFORMATION SECURITY

SUBMITTED BY :-  
MUSKAN MANDLOI  
IT-2K19-34


SUBMITTED TO:-  
DR. SHALIGRAM  
PRAJAPAT SIR



## **Q1. Difference between computer-based information systems and manual systems using clerks and filing cabinets:**

Computer-based information systems and manual systems have different security requirements due to their inherent characteristics:

1. **Complexity:** Computer-based information systems are typically more complex than manual systems. They involve networks, servers, software, and various interconnected components. This complexity introduces a wider range of potential vulnerabilities and threats, requiring sophisticated security measures.
2. **Automation:** Computer-based systems automate processes and store data electronically. This introduces additional security concerns such as data breaches, hacking, and malware. Protection measures like encryption, firewalls, and intrusion detection systems are necessary to safeguard against these threats.
3. **Scale and Accessibility:** Computer-based systems can store and process vast amounts of data, making it easier for threats to exploit vulnerabilities on a larger scale. Additionally, the accessibility of digital information introduces the risk of unauthorized access, requiring stringent access controls and authentication mechanisms.



4.           Physical Security: Manual systems that use clerks and filing cabinets rely on physical security measures to protect sensitive information. Safeguards like locked cabinets, restricted access to documents, and security personnel are crucial. In contrast, computer-based systems require additional measures like secure data centers, backup power supply, and secure server rooms to protect the physical infrastructure.

5.           Data Protection: Both computer-based and manual systems require data protection measures, but the methods differ. Computer-based systems may require encryption, secure transmission protocols, and regular data backups. Manual systems may focus on physical document security, backup copies, and restricted access to filing cabinets.

Overall, computer-based information systems and manual systems have distinct security requirements due to the differences in complexity, automation, scale, accessibility, and data protection measures. Understanding these differences helps in implementing appropriate security controls and safeguards for each type of system.



**Q2. Illustrate the public key implementation of Rivest, Shamir and Adleman with  $p = 7$  and  $q = 11$ .**

Ans :

step 1

the two prime numbers  $p$  and  $q$  are selected as

$$p = 7 \text{ and } q = 11$$

step 2

then the two numbers  $n$  and  $r$  are calculated as

$$n = pq = 7 \times 11 = 77$$

$$r = (p-1)(q-1) = 6 \times 10 = 60$$



step 3

select an integer  $e$

where  $e < r$  and  $e$  has no common factors with  $r$

take  $e = 37$

step 4

calculate the integer  $d$

where  $ed = 1 \bmod r = 1 \bmod (p-1)(q-1)$

$\Rightarrow 37d = 1 \bmod 60$

$\Rightarrow d = 13$

step 5

the decryption key, the secret key is  $(13, 77)$

the encryption key, the public key is  $(37, 77)$

THANKYOU!

