ASSIGNMENT Questions

Introduction:

1. For each of the following assets, assign a low, moderate, or high impact level for the loss of confidentiality, availability, and integrity, respectively. Justify your answers.
    a. An organization managing public information on its Web server.
    b. A law-enforcement organization managing extremely sensitive investigative information.
    c. A financial organization managing routine administrative information (not privacy-related information).
    d. An information system used for large acquisitions in a contracting organization that contains both sensitive, pre-solicitation phase contract information and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.
    e. A power plant contains a SCADA (supervisory control and data acquisition) system controlling the distribution of electric power for a large military installation. The SCADA system contains both real-time sensor data and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.

Symmetric Encryption:

2. Using Feistel cipher, show that decryption is the inverse of encryption.

Changing RSA public keys

3. Suppose MUELE requires every student to have an RSA public key. It also requires that the employee change his or her RSA key at the end of every month.

    a. You just started as a student at Makerere, and your first public key is (n, e) where n is the product of two safe primes, and $e = 3$.
    Whenever a new month starts, you (being lazy) change your public key as little as possible to get by the auditors. What you do, in fact, is just to advance your public exponent e to the next prime number. So, month by month, your public keys look like:

    $$(n, 3), (n, 5)(n, 7), (n, 11), \dots$$

    Explain how your laziness might get you in trouble.

    b. The next year, you try a different scheme.

    In January, you generate a fresh public key (n, e) where n is the product of two primes, p and q.
    In February, you advance p to the next prime p' after p, and q to the next prime q' after q, and set your public key to be (n', e') for a suitable e'.
    Similarly, in March, you advance p' to $p''$and q' to q'', and so on.
    Explain how your new scheme could be broken.

4. Perform encryption and decryption using the RSA algorithm for the following:
   a. $p = 3; q = 11, e = 7; M = 5$
   b. $p = 5; q = 11, e = 3; M = 9$

Digital Signatures

5. When you send an email, it is transmitted through many servers, each of which can potentially modify your message. Luckily we can use public key cryptography to sign our messages, and thereby allow others to verify their integrity. We can also use PKI (like OpenPGP) to safely distribute our public keys.

   Figure out how to send a digitally signed message using your current mail client to your other project team members. Verify the digitally signed messages received from your project team members. If your current mail client doesn't support signatures, you can download and use Thunderbird with the Enigmail extension.

   a. Write up the steps you needed to do the above. (Include a description of your mail client, etc.) What certificates did you have to work with?
   b. Have each member of your team send a digitally signed message to rashida@chalmers.se

Due date is 13th May 2021.