

1. In the class, we have shown a hardware implementation for the AES algorithm and how the hardware components corresponded to the algorithmic components. Please find a paper that describes an implementation of the RSA algorithm and show how the hardware components correspond to the algorithmic components.

- In your opinion, should a cryptographic product manufacturer try to develop an “all in one” product that could perform, for example, DES, AES, and RSA altogether? Why or why not?

2. Try to write a small program that decrypts the following ciphertext – show the program and the results.

mszcx ijddj nzatm lrkdj mlwmc qrktj
tnwir zatnj bxdri amlrs zxrzd dbjbk
wsrir mlrxc icnic qrkza tmlrb cbriz
mlkco mnizx r

- Devise a test for a piece of ciphertext to determine quickly it was likely the result of substitution-only transformation?
- Devise a test for a piece of ciphertext to determine quickly it was likely the result of permutation-only transformation?

3. What characteristic would make an encryption scheme absolutely unbreakable? What characteristics would make it practically unbreakable?

4. What did you learn from Professor Massoud’s talk at the corporate affiliate meeting?

- Please describe why there is interest in analog-to-information and his presentation of his group’s recent progress.
- Describe Prof. Massoud’s philosophy why nano-circuits need to be designed before technology is settled? What is interesting and useful about nano-FPGA?
- Why there is a need for a new technology for interconnects? What are the properties of optical interconnects?