Summary

CSS 322 – Security and Cryptography

What Have You Learnt?

- Theory
  - Encryption
    - Classical techniques
    - Current symmetric key algorithms (DES, AES)
    - Public key algorithms (RSA) and mathematics used
    - Applying algorithms: block modes, where to encrypt
  - Authentication, certificates and digital signatures
  - Hash functions and key distribution
- Practice
  - Applying authentication and digital signatures
  - Security in Internet: IPsec, TLS, Cookies
  - Attacks and defences:
    - Virus, Worms, Denial of Service, Buffer Overflow
    - Firewalls

Well Done!

And good luck in exam and 4th year…