CS3235 Tutorial for week 8
(Sept 29th-Oct 3rd, 2003)

25th September 2003

1. **Question 2, Chapter 9 in textbook:** Decipher the following ciphertext, which was enciphered using the Cæsar cipher: TEBKFKQEBZLROPBLCERJXKBSBKQP.

2. **Question 3, Chapter 9 in textbook:** If one-time pads are provably secure, why are they so rarely used in practice?

3. **Question 1, Chapter 7 in notes:** Differentiate between *block* and *stream* ciphers.

4. **Question 2, Chapter 7 in notes:** In DES, which components of the hardware cause *confusion*, and which *diffusion*?

5. **Question 5, Chapter 7 in notes:** Briefly characterize each of Blowfish, SHA, MD5, RC4, RC5, AES.

6. **Question 6, Chapter 7 in notes:** What is the *timing* attack on RSA?