

CSCI 283 - Computer Security I - Fall 2003
George Washington University

Descrambling, number theory and examples of the use of cryptography

17 September 2003

- A. i. Encrypt the following message using scrambling with a column length of 4:
HOW MANY MILES MUST A MAN WALK ON BEFORE HE CAN CALL HIMSELF MAN
- ii. How would you decrypt the message?
- B. Perform the following mathematical operations using modular arithmetic:
- i. $(5 + 4) \bmod 6$
 - ii. $(5 - 6) \bmod 7$
 - iii. $(3 \times 9) \bmod 5$
 - iv. $(15 \div 3) \bmod 16$
 - v. $3^3 \bmod 7$
 - vi. $\sqrt{2} \bmod 7$
- C. Calculate $5^{37} \bmod 7$ efficiently. How many multiplications did you need?
- D. Write down the sequence of steps in a digital signature creation and verification.
- E. How does a replay attack work when Alice and Bob obtain session keys from a KDC as described in class?
- F. Write down the sequence of steps in a public key authentication protocol.
- G. You are to design the cryptographic protocols for a system for copyright protection using what you have learnt in this class. Design the entire system and describe it concisely.