The University of Newcastle
School of Electrical Engineering and Computer Science

# COMP3260/COMP6360 Data Security

## Week 2 Workshop – 7th March 2019

**1.** Apply Chinese Remainder Theorem to find x in the range [0,59] such that

x mod 4 = 3
x mod 3 = 2
x mod 5 = 4

**2.** Using Chinese Remainder Theorem solve for x in the range [0, n-1].

a) 5x mod 17 = 1
b) 19x mod 26 = 1
c) 17x mod 100 = 1
d) 2x mod 57 =1

**3.** Using extended Euclid's algorithm, find the solution to the equation 17x mod 100 = 1 in the range [0, 99].

**4.** Using Euler's theorem and fast exponentiation, solve the following equation for x in the range [0, n-1].

a) 5x mod 17 = 1
b) 19x mod 26 = 1
c) 17x mod 100 = 1
d) 2x mod 57 =1

**5.** Find the inverse of 5 mod 31.

**6.** Find all solutions to the equation 17x mod 100 = 10 in the range [0, 99].

**7.** Let X be an integer variable represented with 32 bits. Suppose that the probability is ½ that X is in the range $[0, 2^8-1]$, with all such values being equally likely, and ½ that X is in the range $[2^8, 2^{32}-1]$, with all such values being equally likely. Compute H(X).

**8.** Let X be one of the 6 messages: A, B, C, D, E and F, where:
p(A)=p(B)=p(C)=1/4
p(D)=1/8
p(E)=p(F)=1/16
Compute H(X) and find an optimal binary encoding of the message.

**9.** Suppose there are 5 possible messages, A, B, C, D and E, with the probabilities p(A)= 0.5, p(B)= 0.3,p(C)= 0.1, p(D)= 0.05 and p(E)= 0.05. What is the expected number of bits needed to encode these messages in optimal encoding? (That is, find H(M).) Provide optimal encoding.