The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260/COMP6360 Data Security
Week 3 Tutorial
14th and 15th March 2019

1. Find all solutions to the equation 15x mod 25 = 10 in the range [0, 24].

2. Consider GF(2^3) with the irreducible polynomial p(x)=1011 (x^3+x+1). Find additive and multiplicative inverses of all elements of this field.

3. Evaluate complexity of algorithm for fast exponentiation.

4. Evaluate complexity of Euclid's algorithm for finding the greatest common divisor of two integers.

5. Use the Theorem presented in the lecture (see bellow) to explore if there is a simple way to solve '*n* mod *d*' for d=2, 3, 4, 5, 6, 7, 8 and 9. For example, n mod 3 can be found by adding up all the decimal digits of n, and taking mod 3 of the sum.

Theorem: Let *a* and *b* be integers, and let *op* be one of the binary operators +, -, or *. Then *(a op b) mod n = [(a mod n) op (b mod n)] mod n.*

6. Let M be a secret message revealing the recipient of a scholarship. Suppose there were one female applicant, Anne, and three male applicants, Bob, Doug and John. It was initially thought each applicant had the same chance of receiving scholarship; thus p(Anne) = p(Bob) = p(Doug) = p(John) = ¼. It was latter learned that the chances of a scholarship going to a female were ½. Letting S denote the message revealing the sex of the recipient, compute $H_S(M)$.

7. Let M be a 6-digit number in a range [0, 10^6-1] enciphered with Caesar type shifted substitution cipher with key K, $0 \leq K \leq 9$. For example, if K =1, M = 123456 is enciphered as 234567. Compute H(M), H(C), H(K), $H_C(M)$ and $H_C(K)$, assuming all values of M and K are equally likely.

8. Alice rolls two fair dice and records the sum. Bob's task is to ask a sequence of questions with yes/no answers to find out the sum. Help Bob by devising a detailed question strategy that achieves minimum possible ***average*** number of questions.

9. The accuracy of a certain radio station's weather man at predicting rain is given by the following chart.

	Actual rain	Actual no rain
Predicts rain	1/12	1/6
Predicts no rain	1/12	2/3

For example, 1/12 of the time the weatherman predicts rain when in fact it does rain. Notice that the weatherman is correct 3/4 of the time. An uninformed listener observes that he could be correct 5/6 of the time by simply always predicting no rain. He applies for the weatherman's job. However, the station manager declines to hire the listener. Why? Explain using the equivocation of the actual weather condition given the prediction by the weather man, and by the listener.