The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260/COMP6360 Data Security
Workshop Week 3
8th and 10th March 2021

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

2. 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

3. Find the inverse of 5 mod 31.

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

5. 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.

6. Evaluate complexity of algorithm for fast exponentiation.

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

8. 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*

9. 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).

10. 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.

11. 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.

12. 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 $H_S(M)$.

13. Let M be a 6-digit number in a range $[0, 10^6-1]$ enciphered with Caesar type shifted substitution cipher with key K, $0 \le K \le 9$. 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.

14. 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.

15. The accuracy of a certain radio station's weatherman 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 weatherman, and by the listener.