The University of Newcastle
School of Electrical Engineering and Computer Science

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

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

Solution:

gcd(15,25)=5

Since 5 divides 10, the equation 15x mod 25 = 10 has 5 solutions of the form

$x = (2x_0 + 5t) \bmod 25$, t=0,1,2,3,4 where x_0 is the solution to 3x mod 5 =1.

We have $x_0 = 2$ and $x = (4+5t) \bmod 25$, t=0,1,2,3,4:
$x_1 = 4$
$x_2 = 9$
$x_3 = 14$
$x_4 = 19$
$x_5 = 24$

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.

Solution:
GF(2^3) consists of all polynomial with degree at most 2, that is, the following polynomials:
0 0 0
0 0 1
0 1 0
0 1 1
1 0 0
1 0 1
1 1 0
1 1 1

In GF(2^3), the additive inverse of a polynomial *a* is a polynomial *b* such that $a + b = 0\ 0\ 0$. We denote the additive inverse of a by $-a$. Multiplicative inverse of a polynomial a is a polynomial b such that $a \cdot b = 0\ 0\ 1$. We denote the multiplicative inverse of a by a^{-1}.

All elements of GF(2^3) have an additive inverse. For each *a* we obtain $-a$ by subtracting *a* from 0 0 0. Note that in GF(2^3), subtraction is equivalent to bitwise XOR. For example, for $a = 0\ 0\ 0$ we get:

0 0 0
- 0 0 0
---
0 0 0

and thus the additive inverse for *0 0 0* is *0 0 0*.

For $a = 0\ 0\ 1$ we get

0 0 0
- 0 0 1
---
0 0 1

and thus the additive inverse for *0 0 0* is *0 0 1*. In general, for each element of GF(2^3) we have $a = -a$.

All elements of GF(2^3) except *0 0 0* have a multiplicative inverse. To find multiplicative inverse of a: $a\text{-}1 = a^{\varnothing(p(x))-1} \bmod p(x)$, where $\varnothing(p(x)) = 7$ (see lecture notes).

For example, we obtain the multiplicative inverse of 0 0 1 as follows:

$a = 0\ 0\ 1$

$a^{-1} = 0\ 0\ 1^{7-1} \bmod 1011 = 0\ 0\ 1^6 \bmod 1011$

a^2:

0 0 1
× *0 0 1*
---
0 0 1
0 0 0
0 0 0
---
0 0 0 0 1

Thus $a^2 = 0\ 0\ 1$. As $a = a^2$, we have $a = a^2 = a^4 = a^6 = a^{-1} = 0\ 0\ 1$

In the same way we find multiplicative inverses for all elements of GF(2^3). The results are summarized in the following table:

a	-a	a^{-1}
000	000	-
001	001	001
010	010	101
011	011	110
100	100	111
101	101	010
110	110	011
111	111	100

An alternative way to find multiplicative inverses of all elements of GF(2^3) is to construct a multiplication table and read off the multiplicative inverses as a

row and a column having 0 0 1 in their intersection:

	000	001	010	011	100	101	110	111
000	000	000	000	000	000	000	000	000
001	000	***001***	010	011	100	101	110	111
010	000	010	100	110	011	***001***	111	101
011	000	011	110	101	111	100	***001***	010
100	000	100	011	111	110	010	101	***001***
101	000	101	***001***	100	010	111	011	110
110	000	110	111	***001***	101	011	010	100
111	000	111	101	010	***001***	110	100	011

3. Evaluate complexity of algorithm for fast exponentiation.

Solution:
To evaluate the complexity of an algorithm, we first need to identify a barometer statement that is executed at least as many times as any other statement in the algorithm. We can then consider the worst case and provide O (big Oh, of order at most) for the number of times the barometer statement is executed.

```
Algorithm fastexp(a, z, n)
begin "return x = a^z mod n"
 a1:= a; z1 :=z;  x := 1;
 while z1  ≠ 0 do
    begin
      while z1 mod 2 = 0 do
         begin "square a1 while z1 is even"
            z1 := z1 div 2; a1 := (a1*a1) mod n;
         end;
       z1 := z1 - 1; x := (x*a1) mod n;
     end;
  fastexp := x;
end
```

We choose the comparison **z1 mod 2 = 0** in the second while loop as the barometer. statement. This statement is executed once for every 0 and twice for every 1 in the binary representation of the exponent z. In the worst case when we have all 1's, the number of time the barometer statement is executed is $2\times\lceil \log_2 z \rceil = O(\log z)$. Thus we say that the number of steps taken by the algorithms in the worst case is of order at most log z. (Note that we can use the same argument to show the tight bound for both worst and best case: the number of time the barometer statement is executed in the worst case is $2\times\lceil \log_2 z \rceil$, and in the best case is $\lceil \log_2 z \rceil$; since $2\times\lceil \log_2 z \rceil = \Theta(\log z)$, and also $\lceil \log_2 z \rceil = \Theta(\log z)$, we have that the tight bound for worst, best and average case is $\Theta(\log z)$).

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

Solution:
We choose the comparison $g_i \neq 0$ as a barometer statement – see the algorithm bellow.

```
Algorithm gcd(a,n)
begin
g0 := n;
```

```
g1 := a;
i := 1;
while gi ≠ 0 do
  begin
    gi+1 := gi-1 mod gi;
    i := i + 1
  end;
gcd := gi-1
end
```

The barometer statement is executed k-1 times, where n is the index of g such that $g_k=0$ and $g_0, g_1, \ldots, g_{k-1} >0$.
To evaluate k, we first observe that $g_i < g_{i-1}$ and $g_i \le g_{i-2} - g_{i-1}$, for any i>1. For g_i, g_{i+1}, and g_{i+2} where $i \ge 0$, we consider 2 cases:

1. $g_{i+1} \le g_i /2$; since $g_{i+2} < g_{i+1}$, we have $g_{i+2} < g_i /2$
2. $g_{i+1} > g_i /2$; since $g_{i+2} \le g_i - g_{i-1}$, we have $g_{i+2} < g_i /2$

Therefore we always have $g_{i+2} < g_i /2$ and thus the number of binary digits in g_{i+2} is at least one less than the number of binary digits in g_i. It follows that in the worst case $k - 1 \le 2\times \lceil \log_2 g_0 \rceil = O(\log g_0)$.

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*

Solution idea:

d=2; we have $10^0 \bmod 2 = 1$ and $10^k \bmod 2 = 0$ for k >0 . then for any number x with decimal digits $x_k x_{k-1} x_{k-2} \ldots x_0$ we have

$x \bmod 2 = (10^k x_k + 10^{k-1} x_{k-1} + \ldots + 10x_1 + x_0) \bmod 2 =$

$= (10^k x_k \bmod 2 + 10^{k-1} x_{k-1} \bmod 2 + \ldots + 10x_1 \bmod 2 + x_0 \bmod 2) \bmod 2 =$

$= (0 \times x_k \bmod 2 + 0 \times x_{k-1} \bmod 2 + \ldots + 0 \times x_1 \bmod 2 + x_0 \bmod 2) \bmod 2 = (0 \bmod 2 + 0 \bmod 2 + \ldots + 0 \bmod 2 + x_0 \bmod 2) \bmod 2$

$= x_0 \bmod 2$

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 $H_S(M)$.

Solution:

Before the extra knowledge about the sex of the recipient, the probabilities and the entropy were as follows:
p(Anne) = p(Bob) = p(Doug) = p(John) = ¼
$H(M) = \Sigma\ p(M) \log_2 1/p(M) = 4 \times ¼ \times \log_2 4 = 2$ bits

If the sex of the recipient were revealed, the conditional probabilities and the equivocation are as follows:
p(male) = 1/2, p(female) = 1/2
p_{male}(Anne) = 0, p_{male} (Bob) = p_{male} (Doug) = p_{male} (John) = 1/3
p_{female} (Anne) = 1, p_{female} (Bob) = p_{female} (Doug) = p_{female} (John) = 0
$H_S(M) = \Sigma_S\ p(S)\ \Sigma_M\ p_S\ (M) \log_2 1/p_S\ (M) = 1/2 \times (1\times \log_2 1) + 1/2 \times (3 \times 1/3 \times \log_2 3) = 0 + ½ \times \log_2 3 =$ ½ log(3) bits

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, $0 \le K \le 9$. 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.

Solution:
$p(M) = p(C) = 1/10^6$
p(K) = 1/10

$p_C(M) = 1/10$ for the 10 possible messages given ciphertext C
$= 0$ for all other messages

$p_C(K) = 1/10$
(knowing the ciphertext doesn't change the probability of the key)

$H(M) = \Sigma p(M) \log_2 (1/p(M))$
$= 10^6 \times (1/ 10^6) \times \log_2 10^6 = \log_2 10^6 = 6 \log_2 10$

$H(C) = \Sigma\ p(C) \log_2 (1/p(C))$
$= 10^6 \times (1/ 10^6) \times \log_2 10^6 = \log_2 10^6 = 6 \log_2 10$

$H(K) = \Sigma\ p(K) \log_2 1/p(K)$
$= 10 \times (1/10) \times \log_2 10 = \log_2 10$

$H_C(M) = \Sigma\ p(C)\ \Sigma\ p_C(M) \log_2 (1/p_C(M))$

$= 10^6 \times (1/10^6) \times (10 \times (1/10) \times \log_2 10 + (10^6 - 10) \times 0 \times \log_2 (1/0))$
$= \log_2 10$ (because $lim_{x \to 0}\ x \log_2 (1/x) = 0$)

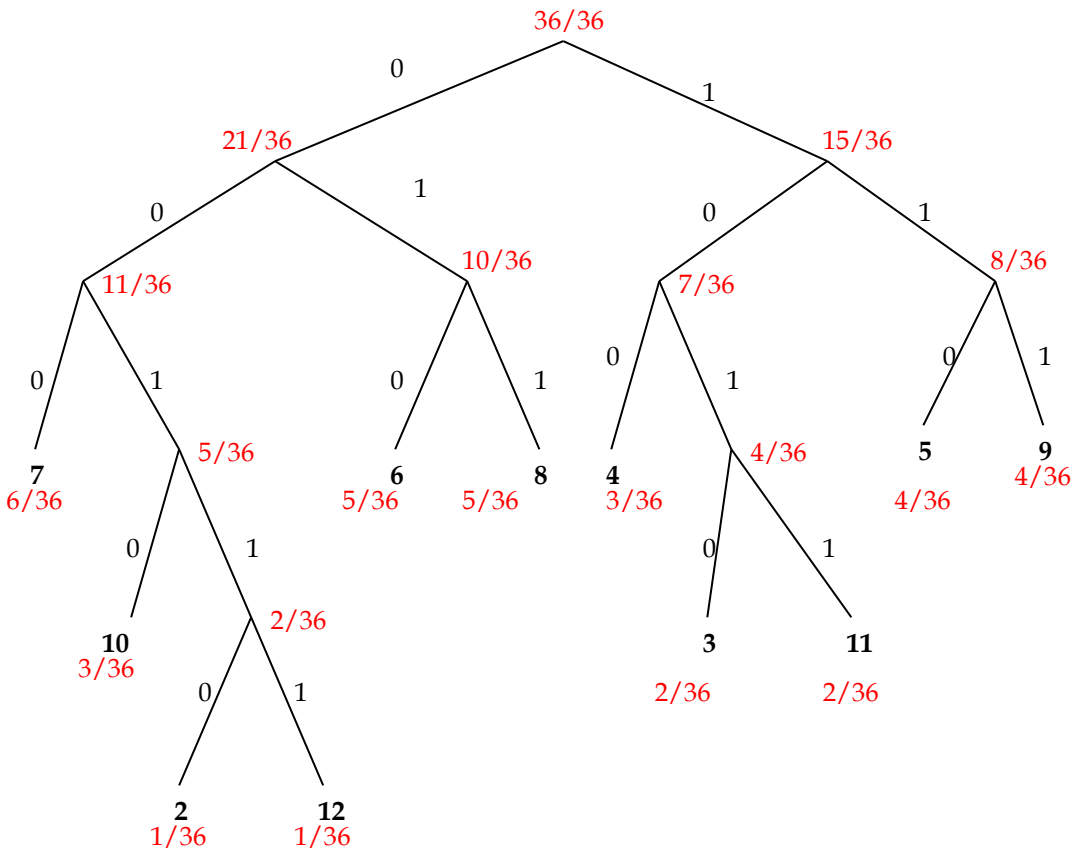
$H_C(K) = \Sigma\ p(C)\ \Sigma\ p_C(K) \log_2 (1/p_C(K))$
$= 10^6 \times (1/10^6) \times (10 \times (1/10) \times \log_2 10) = \log_2 10$

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.

Solution: When rolling two dice we have 36 possible outcomes, and 11 possible sums from 2 to 12. Need to work out the frequency for each sum and this divided by 36 will give the probability of that sum.

p(2) = 1/36	Outcome (1,1)
p(3) = 2/36	Outcomes (1,2) and (2,1)
p(4) = 3/36	Outcomes (1,3), (2,2) and (3,1)
p(5) = 4/36	Outcomes (1,4), (2,3), (3,2) and (4,1)
p(6) = 5/36	Outcomes (1,5), (2,4), (3,3), (4,2) and (5,1)
p(7) = 6/36	Outcomes (1,6), (2,5), (3,4), (4,3), (5,2) and (6,1)
p(8) = 5/36	Outcomes (2,6), (3,5), (4,4), (5,3) and (6,2)
p(9) = 4/36	Outcomes (3,6), (4,5), (5,4) and (6,3)
p(10) = 3/36	Outcomes (4,6), (5,5) and (6,4)
p(11) = 2/36	Outcomes (5,6) and (6,5)
p(12) = 1/36	Outcome (6,6)

To devise the question strategy we create an optimal encoding.



Now we use this encoding to devise the question strategy that will have the minimum possible average number of questions.

Question1: It the sum any of the following; 3, 4, 5, 9 or 11?

Yes: Go to question 2
No: Go to question 6

Question 2: Is the sum either 5 or 9?

Yes: go to question 3
No: go to question 4

Question 3: Is the sum 9?

Yes: Answer is 9.
No: Answer is 5.

Question 4: Is the sum 4?

Yes: Answer is 4.
No: Go to question 5

Question 5: Is the sum 11?

Yes: Answer is 11.
No: Answer is 3.

Question 6: Is the answer either 6 or 8?

Yes: Go to question 7.
No: Go to question 8.

Question 7: Is the answer 8?

Yes: The answer is 8.
No: The answer is 6.

Question 8: Is the answer 7?

Yes: The answer is 7.
No: Go to question 9.

Question 9: Is the answer 10?

Yes: Answer is 10.
No: Go to question 10.

Question 10: Is the answer 12?

Yes: Answer is 12.
No: Answer is 2.

The average number of questions is 3.306.

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.

Solution:

Notation:
Variables: P – prediction; W –weather
p(R) is the probability that it will rain
p(NR) is the probability that it will not rain
p_R(R) is the probability that it will rain, given the prediction that is will rain.
p_{NR}(R) is the probability that it will rain, given the prediction that is will not rain.
p_R(NR) is the probability that it will not rain, given the prediction that is will rain.
p_{NR}(NR) is the probability that it will not rain, given the prediction that is will not rain.

Entropy of the weather when no prediction is known:
p(R) = 1/6
p(NR) = 5/6
$H(W) = \Sigma\, p(W) \log_2 (1/p(W))$
$= (1/6) \times \log_2 6 + (5/6) \times \log_2 (6/5)$
$= (1/6) \times \log_2 3 + (1/6) + (5/6) \times \log_2 3 + (5/6) - (5/6) \times \log_2 5$
$= 1 + \log_2 3 - (5/6) \times \log_2 5$
= 0.650 Bits

The equivocation of the weather when the prediction is known:
a) For the listener.

The probability that the listener predicts rain is 0, and the probability that they predict no rain is 1. The conditional probabilities are as follows.

p_R(R)	0
p_R(NR)	0
p_{NR}(R)	1/6
p_{NR}(NR)	5/6

$H_P(W) = \Sigma\, p(P) \Sigma\, p_P(W) \log_2 (1/p_P(W))$
$= 1 \times ((1/6) \times \log_2 6 + (5/6) \times \log_2 6/5) + 0$
$= (1/6) \times \log_2 3 + (1/6) + (5/6) \times \log_2 3 + (5/6) - (5/6) \times \log_2 5$
$= 1 + \log_2 3 - (5/6) \times \log_2 5$
= 0.650 Bits

Thus knowing the prediction by the listener does not lower the uncertainty about the weather.

b) For the weatherman

The probability that the weatherman predicts rain is 1/4, and the probability that they predict no rain is 3/4. The conditional probabilities are as follows.

$p_R(R)$	(1/12) / ((1/12) + (1/6)) = 1/3
$p_R(NR)$	(1/6) / ((1/12) + (1/6)) = 2/3
$p_{NR}(R)$	(1/12) / ((1/12) + (2/3)) = 1/9
$p_{NR}(NR)$	(2/3) / ((1/12) + (2/3)) = 8/9

$H_P(W) = \Sigma\, p(P)\, \Sigma\, p_P(W)\ \log_2 1/p_P(W)$

$= (1/4) \times ((1/3) \times \log_2 3 + (2/3) \times \log_2 (3/2)) + (3/4) \times ((1/9) \times \log_2 9 + (8/9) \times \log_2 (9/8))$

$= (1/4) \times ((1/3) \times \log_2 3 + (2/3) \times \log_2 3 - (2/3)) + (3/4) \times ((2/9) \times \log_2 3 + (16/9) \times \log_2 3 - (24/9))$

$= (1/4) \times \log_2 3 - (1/6) + (3/2) \times \log_2 3 - 2$

$= (7/4) \times \log_2 3 - (13/6)$

$= 0.607$ Bits.

The equivocation in this case represents the uncertainty of the weather, knowing the prediction. So since the weatherman has a lower equivocation, there is less uncertainty about the weather. He does a better job and should be hired over the novice listener.