Name:_________________

StudentNo:_______________

The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260/COMP6360 Data Security
Supplementary Midterm Test 1

26 March 2021
Test duration: 55 min
100 marks

In order to score marks, you must show all the workings!

STUDENT NUMBER:_______________________

STUDENT NAME:__________________________

PROGRAM ENROLLED:____________________

Question 1	*Question 2*	*Question 3*	*Question 4*	*TOTAL*

$\lg 3 \approx 1.58$
$\lg 5 \approx 2.32$

Name:_________________

StudentNo:________________

1. ***(20 marks)*** Let X be a secret message revealing the recipient of a scholarship. Suppose there were one female applicant, Anne, one non-binary applicant, Robin, and three male applicants, Bob, Doug and John. All applicants have the same chance of receiving scholarship; thus p(Anne) = p(Robin) = p(Bob) = p(Doug) = p(John) = $\frac{1}{5}$. Let Y denote the message revealing the gender of the recipient.
   a. ***(7 marks)*** What is the entropy H(X) of the original messages?
   b. ***(10 marks)*** What is the equivocation $H_Y(X)$ of scholarship recipient given the gender of the recipient?
   c. ***(3 marks)*** By how many bits does knowing the gender reduce the uncertainty about the scholarship recipient?

Show all the workings.

Solution

(a) We use the first letter of each person's name (to make the equations smaller). The entropy of the original message is:

$$\begin{aligned}
H(X) &= p(A)\lg\left(\frac{1}{p(A)}\right) + p(R)\lg\left(\frac{1}{p(R)}\right) + p(B)\lg\left(\frac{1}{p(B)}\right) + p(D)\lg\left(\frac{1}{p(D)}\right) + p(J)\lg\left(\frac{1}{p(J)}\right) \\
&= \frac{1}{5}\lg 5 + \frac{1}{5}\lg 5 + \frac{1}{5}\lg 5 + \frac{1}{5}\lg 5 + \frac{1}{5}\lg 5 \\
&= 5 \times \frac{1}{5}\lg 5 = \lg 5 \approx 2.32
\end{aligned}$$

(b) There are three messages that Y could be: male (M), nonbinary (N), and female (F). We know that:

$$p(F) = \frac{1}{5},\ p(N) = \frac{1}{5},\ \text{and } p(M) = \frac{3}{5}$$

We also know that

$$p_F(Anne) = 1, p_N(Robin) = 1, p_M(Bob) = p_M(Doug) = p_M(John) = \frac{1}{3}$$

and all other conditional probabilities are 0.

We calculate:

$$\begin{aligned}
H_Y(X) &= p(F)\sum_X p_F(X)\lg\left(\frac{1}{p_F(X)}\right) + p(N)\sum_X p_N(X)\lg\left(\frac{1}{p_N(X)}\right) + p(M)\sum_X p_M(X)\lg\left(\frac{1}{p_M(X)}\right) \\
&= p(F)\,p_F(A)\lg\left(\frac{1}{p_F(A)}\right) + p(N)\,p_N(R)\lg\left(\frac{1}{p_N(R)}\right) \\
&\quad + p(M)\left(p_M(B)\lg\left(\frac{1}{p_M(B)}\right) + p_M(D)\lg\left(\frac{1}{p_M(D)}\right) + p_M(J)\lg\left(\frac{1}{p_M(J)}\right)\right) \\
&= \left(\frac{1}{5} \times 1 \times \lg(1)\right) + \left(\frac{1}{5} \times 1 \times \lg(1)\right) + \frac{3}{5}\left(\frac{1}{3}\lg 3 + \frac{1}{3}\lg 3 + \frac{1}{3}\lg 3\right) \\
&= 0 + 0 + \frac{3}{5}\lg 3 = \frac{3}{5}\lg 3 \approx 0.6 \times 1.58 = 0.948
\end{aligned}$$

(c) Knowing the gender reduces the uncertainty by $H(X) - H_Y(X) \approx 2.32 - 0.948 = 1.372$ bits.

$\lg 3 \approx 1.58$

$\lg 5 \approx 2.32$

Name:_________________

StudentNo:_______________

2. ***(28 marks)*** True or false? Justify your answer in a sentence or two.

a. Every integer in the range [1,26] has a multiplicative inverse modulo 27.

b. Equation 5x mod 15 = 1 has more than one solution.

c. Computing in *GF(2^n)* is more time efficient than computing in *GF(p)*, as subtraction and addition are both bitwise exclusive OR.

d. There is no <u>efficient</u> algorithm for computing multiplicative inverses.

e. 100 and 101 are multiplicative inverses in GF(2^3) with irreducible polynomial $p(x) = x^3 + x + 1$.

f. If a language L has 30 letters in its alphabet, absolute rate of L is 4.9.

g. In unconditionally secure ciphers, intercepting ciphertext does not reveal any information about the plaintext or the key

Solution

(a) **False.** Multiples of 3 do not have multiplicative inverses modulo 27.

(b) **False.** There are no solutions to $5x \bmod 15 = 1$: $\gcd(5, 15) = 5$ but that GCD does not divide 1.

Alternatively, observe that the values of $5x$ modulo 15 are $0, 5,$ and 10.

(c) **True.** Adding and subtracting in $GF(p)$ requires tracking carries and reduction mod p, which is not needed for the bitwise OR operation of $GF(2^n)$.

(d) **False.** Euler's Theorem, the Chinese remainder Theorem, and the Euclidean Algorithm can all be used to find multiplicative inverses efficiently. (See question 3).

(e) **False.** $100 \times 101 = 10100$, and after we divide by 1011 we get $10100 - 10110 = 010$ which is not equal to 001.

(f) **True.** The absolute rate of such a language is $\lg 30 \approx 4.9$.

(g) **False.** It is perfectly secure ciphers that reveal no information about plaintext or key. Unconditionally secure ciphers provide insufficient information to uniquely determine the corresponding plaintext, but this is different to offering *no* information.

$\lg 3 \approx 1.58$

$\lg 5 \approx 2.32$

Name:__________________

StudentNo:________________

3. ***(32 marks)*** Find a solution to the equation $7x \bmod 24 = 1$ in the following three ways:

a) (11 marks) Euler's Theorem (by fast exponentiation): $a^{\Phi(n)} \bmod n = 1$, where $gcd(a,n)=1$

Solution:

$7x\ mod\ 24 = 1$

$7^{\phi(24)}\ mod\ 24 = 1$

$7\ x\ 7^{\phi(24)-1}\ mod\ 24 = 1$

$x = 7^{\phi(24)-1}\ mod\ 24 = 1$

$24 = 2^3 \times 3$

$\phi(2^3 \times 3) = 2^{3-1} \times (2-1) \times 3^{1-1} \times (3-1) = 8$

$$\begin{aligned} x &= 7^{\phi(24)-1} mod\ 24 \\ &= 7^7\ mod\ 24 \\ &= 7\ x\ 7^6\ mod\ 24 \\ &= 7\ x\ 49^3\ mod\ 24 \\ &= 7\ x\ 1^3\ mod\ 24 \\ &= 7\ mod\ 24 \\ &= 7 \end{aligned}$$

Name:__________________

StudentNo:________________

b) (11 marks) Chinese Remainder Theorem: Let $d_1, \ldots, d_t$ be pairwise relatively prime, and let $n = d_1 \times \ldots \times d_t$. Then the system of equations $x \bmod d_i = x_i$ $(i = 1, \ldots, t)$ has a common solution x in the range $[0, n-1]$. The common solution is

$$x = \sum_{i=1}^{t} \frac{n}{d_i} y_i x_i \bmod n$$

where y_i is a solution of $(n/d_i)\, y_i \bmod d_i = 1$, $i = 1, \ldots, t$.

Solution:

$24 = 2^3 \times 3 = 3 \times 8$

$7x_1 \bmod 3 = 1 \rightarrow x_1 \bmod 3 = 1 \rightarrow x_1 = 1$

$7x_2 \bmod 8 = 1 \rightarrow x_2 \bmod 8 = 7 \rightarrow x_2 = 7$

$d_1 = 3, \qquad x_1 = 1$

$d_2 = 8, \qquad x_2 = 7$

$\frac{3 \times 8}{3} y_1 mod\ 3 = 1$

$8\, y_1\ mod\ 3 = 1$

$(8\ mod\ 3 \times y_1\ mod\ 3)\ mod\ 3 = 1$

$2 \times y_1\ mod\ 3 = 1$

$y_1 = 2$

$\frac{3 \times 8}{8} y_2\ mod\ 8 = 1$

$3\, y_2\ mod\ 8 = 1$

$y_2 = 3$

$$x = \left(\frac{3x8}{3} \times 2 \times 1 + \frac{3x8}{8} \times 3 \times 7\right) mod\ 24$$
$$= (16 + 63)\ mod\ 24 = (16 + 15)\ mod\ 24 = 31\ mod\ 24 = 7$$

lg 3 ≈ 1.58
lg 5 ≈ 2.32

c) (10 marks) Extended Euclid's algorithm:

```
Input: a, n
Output: None
inv(a,n) {
      g[0] = n; g[1] = a
      u[0] = 1; u[1] = 0
      v[0] = 0; v[1] = 1
      i = 1
      while (g[i] ≠  0) // "g[i] = u[i]n + v[i]a"
      {
            y = g[i-1] / g[i]  //integer division
            g[i+1] = g[i-1] – y × g[i]
            u[i+1] = u[i-1] – y × u[i]
            v[i+1] = v[i-1] – y × v[i]
            i = i +1
      }
      if v[i-1] ≥ 0 then  return v[i-1] else return v[i-1] + n
}
```

For this part, it is sufficient to fill in the table below tracing the algorithm and circle the solution:

i	y	g[i]	u[i]	v[i]
0		24	1	0
1		7	0	1
2	3	3	1	-3
3	2	1	-2	7
4	3	0	7	-24

Name:_________________

StudentNo:_______________

4. ***(20 marks)*** Let *a=111*. If *GF(2³)* with irreducible polynomial $p(x)= x^3 + x^2 + 1$, use Euler's theorem to find a^{-1} and then verify that $a\times a^{-1} \bmod p(x)=1$.

Solution

We know that $a^{\phi(p(x))} \bmod p(x) = 1$ which we can write as

$$a \times a^{\phi(p(x))-1} \bmod p(x) = 1$$

and so $a^{\phi(p(x))-1}$ must be the inverse of a. We know[†] that $\phi(p(x)) = 7$ and so the inverse must be a^6.

To calculate a^6 with fast exponentiation we have

$$a^{-1} = a^6 \bmod p(x) = \left(a^2\right)^3 \bmod p(x) = a^2 \times \left(a^2\right)^2 \bmod p(x)$$

So we first calculate a^2, then from that calculate a^4, and from those we can calculate a^6.

a^2 :

$$\begin{array}{r} 111\times \\ 111 \\ \hline 111 \\ 111 \\ 111 \\ \hline 10101 \end{array}$$

We must divide by $p(x)$ and find the remainder

$$\begin{array}{r} 10101- \\ 1101 \\ \hline 1111- \\ 1101 \\ \hline 010 \end{array}$$

So $a^2 = 010$.

a^4 :

$$\begin{array}{r} 010\times \\ 010 \\ \hline 000 \\ 010 \\ 000 \\ \hline 00100 \end{array}$$

We do not need to divide by $p(x)$ in this case, because the product only has 3 significant bits

So $a^4 = 100$

a^6 :

$$\begin{array}{r} 010\times \\ 100 \\ \hline 000 \\ 000 \\ 010 \\ \hline 1000 \end{array}$$

We must divide by $p(x)$ and find the remainder

$$\begin{array}{r} 1000- \\ 1101 \\ \hline 101 \end{array}$$

So the inverse is 101.

We check that $a \times a^{-1} \bmod p(x)$ is indeed equal to 1 like it should be.

$$\begin{array}{r} 111\times \\ 101 \\ \hline 111 \\ 000 \\ 111 \\ \hline 11011 \end{array}$$

We must divide by $p(x)$ and find the remainder

$$\begin{array}{r} 11011- \\ 1101 \\ \hline 001 \end{array}$$

The multiplication results in 001 like it should, so we have confirmed that 101 is the inverse of 111 (in GF(2^3) with irreducible polynomial $p(x) = x^3 + x^2 + 1$).

[†]Know because $p(x) = x^3 + x^2 + 1$ is an irreducible polynomial, and so every non-zero polynomial with degree less than 3 is relatively prime to it. There are 7 polynomials.

$\lg 3 \approx 1.58$

$\lg 5 \approx 2.32$