Solutions to Comp3260/Comp6460 Data Security Midterm Test 1

1. Let M be a secret message revealing the recipient of a scholarship. Suppose there were one female applicate: Anne, and three male applicants: Bob, Doug, and John. It was initially thought each applicant had the same chance of receiving the scholarship; thus $p(\textbf{Anne}) = p(\textbf{Bob}) = p(\textbf{Doug}) = p(\textbf{John}) = \frac{1}{4}$. It was later learned that the chances of a scholarship going to a female were $\frac{1}{2}$. Letting S denote the message revealing the sex of the recipient, compute $H_S(M)$.

The message S will be either Male or Female, which we will denote by *Ma* and *Fe* respectively. We are given that $p_{Fe} = \frac{1}{2}$. and from this can conclude that $p_{Ma} = \frac{1}{2}$. Assuming that Bob, Doug and John are all equally likely if a male candidate is chosen, we have the following conditional probabilities:

$$p_{Ma}(\text{Bob}) = p_{Ma}(\text{Doug}) = p_{Ma}(\text{John}) = \frac{1}{3} \qquad p_{Ma}(\text{Anne}) = 0$$
$$p_{Fe}(\text{Bob}) = p_{Fe}(\text{Doug}) = p_{Fe}(\text{John}) = 0 \qquad p_{Fe}(\text{Anne}) = 1$$

We now have everything we need to calculate $H_S(M)$. Let $\sigma := \{Ma, Fe\}$ and $\mu := \{\text{Alice}, \text{Bob}, \text{Doug}, \text{John}\}$. Note that for the purposes of this computation, $0 \log_2(0^{-1}) = 0$ despite the division by zero in the log (we can justify this by considering $\lim_{x\to 0^+} x \log_2(x^{-1}) = 0$)

$$\begin{aligned}
H_S(M) &= \sum_{S\in\sigma} \left(p(S) \sum_{K\in\mu} p_S(K) \log_2 \left(p_S(k)^{-1}\right) \right) \\
&= p(Ma) \sum_{K\in\mu} p_{Ma}(K) \log_2 \left(p_{Ma}(K)^{-1}\right) + p(Fe) \sum_{K\in\mu} p_{Fe}(K) \log_2 \left(p_{Fe}(K)^{-1}\right) \\
&= \frac{1}{2} \left(0 \log_2(0^{-1}) + \frac{1}{3} \log_2(3) + \frac{1}{3} \log_2(3) + \frac{1}{3} \log_2(3) \right) + \frac{1}{2} \left(1 \log_2(1) + 0 \log_2(0^{-1}) + 0 \log_2(0^{-1}) + 0 \log_2(0^{-1}) \right) \\
&= \frac{1}{2} \left(0 + 3 \cdot \frac{1}{3} \log_2(3) \right) + \frac{1}{2} (0) \\
&= \frac{1}{2} \log_2(3) \approx 0.5 \cdot 1.58 = 0.79
\end{aligned}$$

2. True or false?

a. Every integer in the range $[1, 28]$ has a multiplicative inverse modulo 29.
True: 29 is a prime number so $GF(29)$ is a field and every non-zero element of a field is invertible.

b. Every integer in the range $[1, 21]$ except 2 and 11 has a multiplicative inverse modulo 22.
False: Any number a for which $\gcd(a, 22) \neq 1$ has no inverse modulo 22. So 4 in particular has no multiplicative inverse modulo 22 (because $\gcd(4, 22) = 2 \neq 1$) and neither does $6, 8, 10, 12, 14, 16, 18$, and 20.

c. Equation $3x \bmod 15 = 1$ has more than one solution.
False: $3x \bmod 15 = 1$ has no solutions ($\gcd(3, 15) = 3$ which does not divide 1 so there are no solutions).

d. Equation $3x \bmod 15 = 9$ has exactly one solution.
False: There are several solutions: $x = 3$, $x = 8$, and $x = 13$ ($\gcd(3, 15) = 3$ which divides 9 so there are 3 solutions).

e. Computing in $GF\left(2^3\right)$ is less efficient than computing in $GF(p)$, as p is a prime number.
False: Computing in $GF(2^n)$ is more efficient than computing in $GF(p)$ where $2^{n-1} < p < 2^n$.

f. There is no efficient algorithm for computing greatest common divisors.
False: The extended euclidean algorithm is an efficient algorithm for computing greatest common divisors.

g. There exists an efficient algorithm for computing Euler's totient function.
False: Such an algorithm would require an efficient factorisation algorithm which does not exist.

h. There exists an efficient algorithm for computing a common solution of the system of equations of the form $x \bmod d_i = x_i$, $1 \leq i \leq k$, where d_i's are pairwise relatively prime.
True: The chinese remainder theorem is an efficient algorithm for computing such a common solution.

i. 100 and 110 are multiplicative inverses in $GF\left(2^3\right)$ with irreducible polynomial $p(x) = x^3 + x + 1$.
False: $100 \cdot 110 \bmod p(x) = 10$ which is not 1, so 100 and 110 are not multiplicative inverses of each other modulo $p(x)$.

j. 101 and 111 are additive inverses in $GF\left(2^3\right)$ with irreducible polynomial $p(x) = x^3 + x + 1$.
False: $101 + 111 = 10$ which is not 0, so 101 and 111 are not additive inverses of each other.

3. Find a solution to the equation $3x \bmod 20 = 1$ ***in the following 3 ways:***

Note that the correct answer to this problem is $x = 7$ *which can be easily verified (* $3 \cdot 7 \bmod 20 = 21 \bmod 20 = 1$*). This is included as a reference for the following solutions.*

a) Euler's Theorem (by fast exponentiation)

We have $a = 3$ and $n = 20$. Since $\gcd(3, 20) = 1$ we can use Euler's theorem. We know from the theorem that

$$3^{\Phi(20)} \bmod 20 = 1 \implies 3 \cdot 3^{\Phi(20)-1} \bmod 20 = 1$$

so it must be the case that $x = 3^{\Phi(20)-1} \bmod 20$.

To compute $\Phi(20)$ we first note that $20 = 2^2 \cdot 5$ so

$$\Phi(20) = 2^{2-1} \cdot (2-1) \cdot (5-1) = 2 \cdot 1 \cdot 4 = 8$$

we may now use the fast exponentiation algorithm to compute $x = 3^7 \bmod 20 = 7$ (see Figure 1).

Note that instead of using the pseudocode algorithm from the notes, we can perform an equivalent computation:

$$\begin{aligned} 3^7 \bmod 20 &= \left(3 \cdot 3^6\right) \bmod 20 = \left(3 \cdot 9^3\right) \bmod 20 = \left(3 \cdot 9 \cdot 9^2\right) \bmod 20 \\ &= (27 \cdot 81) \bmod 20 = (7 \cdot 1) \bmod 20 = 7 \end{aligned}$$

b) Chinese Remainder Theorem

We know that $20 = 2 \cdot 2 \cdot 5 = 4 \cdot 5$, so we choose $d_1 = 4$ and $d_2 = 5$. We find x_1 and x_2 by solving:

$$\begin{aligned} 3x_1 \bmod d_1 = 1 &\implies 3x_1 \bmod 4 = 1 \\ 3x_2 \bmod d_2 = 1 &\implies 3x_2 \bmod 5 = 1 \end{aligned}$$

Which has solution $x_1 = 3$ and $x_2 = 2$. We therefore have the system of equations

$$\begin{aligned} x \bmod d_1 = x_1 &\implies x \bmod 4 = 3 \\ x \bmod d_2 = x_2 &\implies x \bmod 5 = 2 \end{aligned}$$

Which has common solution

$$x = \left(\frac{20}{d_1} y_1 x_1 + \frac{20}{d_2} y_2 x_2\right) \bmod 20$$

where

$$\begin{aligned} \left(\frac{20}{d_1} \cdot y_1\right) \bmod d_1 = 1 &\implies 5y_1 \bmod 4 = 1 \\ \left(\frac{20}{d_2} \cdot y_2\right) \bmod d_2 = 1 &\implies 4y_2 \bmod 5 = 1 \end{aligned}$$

Which has solution $y_1 = 1$ and $y_2 = 4$. So

$$\begin{aligned} x &= \left(\frac{20}{d_1} y_1 x_1 + \frac{20}{d_2} y_2 x_2\right) \bmod 20 \\ &= (5 \cdot 1 \cdot 3 + 4 \cdot 4 \cdot 2) \bmod 20 = (15 + 32) \bmod 20 = (15 + 12) \bmod 20 \\ &= 27 \bmod 20 = 7 \end{aligned}$$

c) Extended Euclidean algorithm Applying the algorithm provided gives the table of values seen in Figure 1.

a	z	x
3	7	1
3	6	3
9	3	3
9	2	7
1	1	7
1	0	**7**

i	y	g	u	v
0	-	20	1	0
1	-	3	0	1
2	6	2	1	-6
3	1	1	-1	**7**
4	2	0	n/a	n/a

Figure 1: Fast Exponentiation Algorithm (left) and Extended Euclidean Agorithm (right)

4. Let $a = 101$ in $GF\left(2^3\right)$ with irreducible polynomial $p(x) = x^3 + x^2 + 1$. Use Euler's theorem to find $a^{-}1$ and then verify that $a \times a^{-}1 \bmod p(x) = 1$.

Because $p(x)$ is irreducible, and $GF(2^3)$ has 8 elements it must be that $\Phi(p(x)) = 2^3 - 1 = 7$. By Euler's theorem:

$$a^{\Phi(p(x)} \bmod p(x) = 1 \implies \left(a \cdot a^{\Phi(p(x)-1)}\right) \bmod p(x) = 1 \implies a^{-1} = a^{\Phi(p(x)-1)} \bmod p(x)$$

so

$$\begin{aligned} a^{-1} &= a^6 \bmod p(x) = \left(a^2 \cdot a^4\right) \bmod p(x)) \\ &= (110 \cdot (110 \cdot 110)) \bmod p(x) = (110 \cdot 11) \bmod p(x) \\ &= 111 \end{aligned}$$

The working for $a^2 = 110$, $a^4 = a^2 \cdot a^2 = 11$, $a^6 = a^2 \cdot a^4 = 111$, and the check that $aa^6 = 1$ is as follows:

$$a^2 \quad \begin{array}{r} 101 \times \\ \underline{101} \\ 101 \\ 000 \\ \underline{101} \\ 10001 \end{array} \qquad a^4 \quad \begin{array}{r} 110 \times \\ \underline{110} \\ 000 \\ 110 \\ \underline{110} \\ 10100 \end{array} \qquad a^6 \quad \begin{array}{r} 110 \times \\ \underline{11} \\ 110 \\ \underline{110} \\ 1010 \end{array} \qquad a^6 a \quad \begin{array}{r} 111 \times \\ \underline{101} \\ 111 \\ 000 \\ \underline{111} \\ 11011 \end{array}$$

$$\begin{array}{r} 11 \\ 1101\overline{)10001} \\ \underline{1101} \\ 1011 \\ \underline{1101} \\ 110 \end{array} \qquad \begin{array}{r} 11 \\ 1101\overline{)10100} \\ \underline{1101} \\ 1110 \\ \underline{1101} \\ 11 \end{array} \qquad \begin{array}{r} 1 \\ 1101\overline{)1010} \\ \underline{1101} \\ 111 \end{array} \qquad \begin{array}{r} 1 \\ 1101\overline{)11011} \\ \underline{1101} \\ 1 \end{array}$$

5. Give a definition and provide a formula for each of the following terms:

a. Entropy

Entropy is the average number of bits needed to encode all possible messages in an optimal encoding. The entropy of a message measures its uncertainty: it gives the number of bits of information that must be learned when the message has been distorted by a noisy channel or hidden in cyphertext.

$$H(X) = \sum_{i=1}^{n} p(x_i) \log_2 \left(p(x_i)^{-1}\right)$$

b. Equivocation

Equivocation measures the entropy of a message, X, given some additional information, Y. It is the uncertainty about X given the knowledge Y. In other words, equivocation is the conditional entropy of X given Y.

$$H_Y(X) = \sum_Y p(Y) \sum_X p_Y(X) \log_2 \left(p_Y(X)^{-1}\right)$$

c. Perfect secrecy

Perfect secrecy is defined by the condition

$$p_C(M) = p(M)$$

where $p_C(M)$ is the conditional probability that message M was sent given cyphertext C was received. Perfect secrecy is achieved if no matter how much ciphertext is intercepted, nothing can be learned about the plaintext.

A necessary and sufficient condition for perfect secrecy is

$$p_M(C) = p(C) \text{ for all messages } M \text{ and all cyphertexts } C$$

so the probability of receiving a particular cyphertext C given that M was sent is the same as the probability of receiving C given that any other message M' was sent.