CIS 3362 Final Exam Review Solutions

1) Decrypt the following ciphertext that was encrypted using the shift cipher:

```
Mubsecujejxuvydqbunqc
```

Solution
Try each shift one by one on the first 4 letters and see if anything looks like English. I will shift forward instead of backwards until I see something promising:

```
0  mub    1  nvc    2  owd    3  pxe    4  qyf    5  rzg
6  sah (maybe?)     7  tbi    8  ucj    9  vdk
10 wel (this looks better, try this first)
So, maybe the encryption key was 16, so to decrypt we subtract
16 or add 10:
```

welcome to the final exam

2) Consider the two following sets of letter frequencies:

Frequency	A	B	C	D	E	F
Set 1	6	19	23	10	15	27
Set 2	26	8	16	26	4	20

Find the mutual index of coincidence between the two sets. **Express your answer as a fraction in lowest terms.**

Solution

$$MIC = \frac{6 \times 26 + 19 \times 8 + 23 \times 16 + 10 \times 26 + 15 \times 4 + 27 \times 20}{100 \times 100} = \frac{1536}{10000} = \frac{384}{2500} = \mathbf{\frac{96}{625}}$$

3) Consider a Diffie-Hellman key exchange with p = 83 and g = 13. Let Alice's secret key be 12 and Bob's secret key be 15. What is the shared secret key that they exchange, in between 0 and 82, inclusive? (Please write what calculations you made on your calculator.)

Solution
It's good enough to calculate what Alice would do. She receives 13^{15} mod 83 from Bob. To calculate this with a calculator, one way we could do it is calculate $13^5 = 371293$ and mod this by 83, to yield 34. Then, we can just take $34^3 = 39304$ and mod this by 83 to get 45.

Alice then calculates $45^{12} = (45^4)^3$ mod 83. To do this calculation, let's first calculate $45^4 = 4100625$ and mod it by 83 to get 10. Finally, we can take $10^3 = 1000$ and mod by 83 to get **4,** their shared key.

4) What is the ciphertext produced when using the Hill cipher to encrypt the plaintext "RESTED" using the key $\begin{bmatrix}13 & 11 & 3\\ 4 & 22 & 17\\ 19 & 16 & 5\end{bmatrix}$?

Solution

$$\begin{bmatrix}13 & 11 & 3\\ 4 & 22 & 17\\ 19 & 16 & 5\end{bmatrix}\begin{bmatrix}17\\ 4\\ 18\end{bmatrix} = \begin{bmatrix}13\times 17 + 11\times 4 + 3\times 18\\ 4\times 17 + 22\times 4 + 17\times 18\\ 19\times 17 + 16\times 4 + 5\times 18\end{bmatrix} = \begin{bmatrix}319\\ 462\\ 477\end{bmatrix} \equiv \begin{bmatrix}7\\ 20\\ 9\end{bmatrix}, \text{ so RES} \rightarrow \text{HUJ}$$

$$\begin{bmatrix}13 & 11 & 3\\ 4 & 22 & 17\\ 19 & 16 & 5\end{bmatrix}\begin{bmatrix}19\\ 4\\ 3\end{bmatrix} = \begin{bmatrix}13\times 19 + 11\times 4 + 3\times 3\\ 4\times 19 + 22\times 4 + 17\times 3\\ 19\times 19 + 16\times 4 + 5\times 3\end{bmatrix} = \begin{bmatrix}300\\ 215\\ 440\end{bmatrix} \equiv \begin{bmatrix}14\\ 7\\ 24\end{bmatrix}, \text{ so TED} \rightarrow \text{OHY}$$

5) Recall that a primitive root of a prime, p, is an integer a ($1 \leq a \leq p-1$) such that *the smallest* positive integer e such that $a^e \equiv 1 \pmod p$ is p-1. In particular, this result also means that the values $a^1, a^2, a^3, ..., a^{p-1} \bmod p$ are all distinct and form the set {1, 2, 3, ..., p-1}. Given that 13 is a primitive root mod 19, determine all of the other primitive roots mod 19. (Note: The intention here is NOT for you to try all of the other values by exponentiating them. There is a much faster way to do this and you're being graded on discovering that way. Since you have a calculator at your disposal, please do simplify your answers to be in between 1 and 18, inclusive. Also, more blanks than necessary are provided below so as to not give away the number of answers.)

Solution

Note that if a is a primitive root and k shares a common factor, d, d > 1, with p-1, then a^k can't be a primitive root because we have for $x = \frac{p-1}{d}$, $(a^k)^x \equiv a^{c(p-1)} \equiv 1\ (mod\ p)$, for some integer c. Similarly, if k doesn't share a common factor with p-1, there is no exponent x smaller than p-1 for which $(a^k)^x \equiv 1\ (mod\ p)$. (This was shown in class previously.) Thus, since we know 13 is a primitive root of 19, and we also know that 5, 7, 11, 13, and 17 are the only values (other than 1) to not share a common factor with 18, the other primitive roots of 19 are 13^5, 13^7, 13^{11}, 13^{13} and $13^{17} \bmod 19$. We can just use repeated multiplication to determine each of these as follows:

$13^2 \equiv 169 \equiv 17 \equiv -2 \pmod{19}$
$13^4 \equiv (13^2)^2 \equiv (-2)^2 \equiv 4 \pmod{19}$
$13^8 \equiv (13^4)^2 \equiv (4)^2 \equiv 16 \equiv -3 \pmod{19}$
$13^{16} \equiv (13^8)^2 \equiv (-3)^2 \equiv 9 \pmod{19}$

Now, use these results to determine each of our other primitive roots:
$13^5 \equiv 13^4 13^1 \equiv (4)(13) \equiv 52 \equiv 14 \pmod{19}$
$13^7 \equiv 13^4 13^2 13^1 \equiv (4)(-2)(-6) \equiv 48 \equiv 10 \pmod{19}$
$13^{11} \equiv 13^8 13^2 13^1 \equiv (-3)(-2)(-6) \equiv -36 \equiv 2 \pmod{19}$
$13^{13} \equiv 13^8 13^4 13^1 \equiv (-3)(4)(-6) \equiv 72 \equiv 15 \pmod{19}$
$13^{17} \equiv 13^{16} 13^1 \equiv (9)(13) \equiv 117 \equiv 3 \pmod{19}$

Thus, the 5 other primitive roots of 19 are **2, 3, 10, 14 and 15.**

6) Alice and Bob want to exchange 1024 bits for a set of secret keys via Quantum Cryptography. Alice plans on sending bits to Bob, randomly picking the orientation of her reader, with Bob not knowing, so that they can detect any intruder. They would like a probability of 2^{-100} that an intruder could successfully read all the bits sent without being detected. Recall that after sending the bits, Alice and Bob "sample" some of the bits and check which readers they used, verifying that the exchange was secure if all of the bits for which they used the same reader in their sample were correctly interpreted by Bob. Roughly how many bits must Alice send originally, to give Alice and Bob at least a 50% chance of having exchanged 1024 bits while making the chance that an intruder intercepted the bits roughly 2^{-100}? (Note: A range of answers will be accepted for this question, but an answer that is artificially high will lose credit. Full credit will only be given for work that justifies the answer.)

Solution

The 1024 bits represent bits NOT initially sampled for which the guesses were correct. Thus, we need 2048 unsampled bits (roughly) to ensure 1024 of them were properly exchange.

Now, we must add on the sampled bits. We want the intruder's chance of succeeding to be roughly 2^{-100}. This means we want to have 100 sampled bits where Alice and Bob guessed correctly, but the intruder did not. This translates to roughly 200 sampled bits where Alice and Bob guessed correctly, since the intruder will also go along with them 1/2 the time. But, to get 200 sampled bits correct between Alice and Bob, we really need 400 sampled bits total.

Thus, our total bit count is 2048 (unsampled) + 400 (sampled) = 2448.

In terms of grading, any answer in between 2400 and 2600 will be accepted.

7) One year on Venus is 225 days. What is the probability that of a random sample of 10 Venetians, all of them have different birthdays? Please use a calculator and determine the probability rounded to the nearest thousandth.

Solution

Product Notation: $\prod_{i=0}^{9} \frac{225-i}{225}$

Approximate Value of Desired Probability: **0.816**