Juan Chavez
CS165
Hw1

CS165 – Computer Security

1. The file book1.enc is an encrypted version of one of the books from Project Gutenberg (www.gutenberg.org). It was encrypted using a stream cipher whose key stream was taken from the output of a linear congruential random number generator. Specifically, each character of the plaintext (encoded using UTF-8) was converted into an integer, and then that integer was added with the corresponding output from the LCG. Each line of book1.enc contains the encrypted version of a single character from the plaintext. Decrypt book1.enc, and provide the parameters of the random number generator (including the seed).

book1.enc was Alice's Adventures in Wonderland. The following are the values I came up with:

The LCG function is : x[n] = (4276115653*x[n-1] + 634785765) mod(4294967296)
Seed: 4313902048
(I tried calculating for the seed but I fell short for some reason, so I used the number following the seed to decrypt it)

We were given the cribbing phrase "Project Gutenberg." Which would give us a sequential group of values belonging to the keystream after we took the ciphertext integer and subtracted the ASCII numerical equivalent for each corresponding letter.

Manipulating the LCG equation to rid ourselves of a and b we found a formula that allowed us to solve for integers (albeit large ones) that had to be multiples of m (i.e. were equal to 0modm). This implied that m was contained in this large integer. To simplify the calculation, I solved for five cases of these large integers that had a congruency of 0modm and took their aggregate GCD, thus narrowing down the value of m. Assuming a sufficient amount of reducing had been done, I used the obtained GCD and treated it as it were m, solved for a and b, and tried generating the keystream, which matched the values we previously solved for. After this, it was only a matter of generating the keystream, subtracting their values from the ciphertext, and outputting their character equivalents on another file, which rendered the decrypted version of the book.

2. The file book2.enc is also an encrypted version of one of the books from Project Gutenberg. This time, it was encrypted using a combination of two ciphers. The first was a mono-alphabetic substitution cipher. The second was a columnar transposition cipher. Decrypt book2.enc. Provide the number of columns that were used in the transposition cipher.

With this combination, it becomes a matter of first decrypting the substitution and then undoing the transposition cipher.
Decrypting the substitution reduces to the English language's character frequency analysis. After having replaced the unknown symbols with what they most likely represent, we were to undo the columnar transposition cipher.

Juan Chavez
CS165
Hw1

3. Prove: For all $n \geq 3$, $\varphi(n)$ is even.

Preliminary proof:

$\varphi(p^q) = p^q - p^{q-1}$

Since the only numbers between 1 and p^q that are not relatively prime to p^q are those which are divisible by p, we can deduce that there are p^q/p of these, in other words p^q/p is equivalent to p^{q-1} subtracting this from φ we get the result above.

There are two cases for n, when it is even and when it is odd.

For the first case, when n is even (i.e. n is a power of two or $n = 2^q$), applying the definition of φ(n) we get $2^q - 2^{q-1}$ which remains an even number.

For the second case, n is odd (i.e. n is not a power of two), which implies there exists an odd prime p and an integer q (such that q is not zero, since everything is divisible by one) where $p^q \mid n$ (i.e. divides n) and $p^{q+1} \nmid n$ (i.e. does not divide n). Therefore, we can write $n = p^q k$ (i.e. n is a multiple of p^q). Because of the multiplicative properties of φ(n) we can write that $\varphi(n) = \varphi(p^q) * \varphi(k)$ which is equivalent to $\varphi(n) = p^{q-1} * (p-1) * \varphi(k)$, and since p is odd, $\varphi(n)$ will be even.

4. Prove: If $m \perp n$, then $n^{\varphi(m)} + m^{\varphi(n)} \equiv 1 \pmod{mn}$

By Euler's extension of Fermat's 'Little' Theorem, we get that:

$m^{\varphi(n)} \equiv 1 mod(n)$

$n^{\varphi(m)} \equiv 1 mod(m)$

this implies:

$m^{\varphi(m+n)} \equiv 1 mod(n)$

$n^{\varphi(m+n)} \equiv 1 mod(m)$

Since the gcd(m,n) is 1, we can write that

$n^{\varphi(m)} + m^{\varphi(n)} \equiv 1 mod(mn)$

5. Prove: If $a \perp n$, then $a^{\varphi(n)-1} + a^{\varphi(n)-2} + \ldots + a^2 + a + 1 \equiv 0 \pmod{n}$

By definition, a geometric summation has the form:

$$1 + Q + Q^2 + \ldots + Q^k \equiv \sum_{i=0}^{k} Q^i \equiv \frac{Q^{K+1}-1}{Q-1}$$

In the case of a and n, we can write this as:

$$a^{\varphi(n)-1} + a^{\varphi(n)-2} + \ldots + a^2 + a + 1 \equiv \sum_{i=0}^{\varphi(n)-1} a^i \equiv \frac{a^{\varphi(n)-1+1}-1}{a-1} mod(n)$$

Applying Fermat's Little Theorem on $a^{\varphi(n)-1+1} \equiv a^{\varphi(n)}$ (i.e. the first term in the fraction) because a and n meet the requirement of being coprime, we get that:

$a^{\varphi(n)} \equiv 1 mod(n)$.

This implies that the geometric summation above is equivalent to:

$\frac{1-1}{a-1} mod(n) \equiv 0 mod(n)$