Theory Homework Assignment 2

Student Name: - Tolulope Olugbenga
Student Number: - 3643581

Questions/ Answers

1a.) p is a prime number, if $a^p \equiv b^p \ mod \ p$ then prove that $a^p \equiv b^p \ mod \ p^2$?

By Fermat $p \mid a-b$, then $a \equiv b$ in modulo p

$$\frac{a^p - b^p}{a-b} = \left(a^{p-1} + a^{p-2}b + \cdots b^{p-2}a + b^{p-1}\right) \equiv \left(b^{p-1} + b^{p-2}b + \cdots b^{p-2}b + b^{p-1}\right) \equiv pb^{b-1} \equiv 0$$

In modulo p

Since $\frac{a^p - b^p}{a-b}$ and $a-b$ are divisible by p. The product $a^p - b^p$ is divisible by p^2.

1b.) Let $gcd(m,n)=1$, then prove that $m^{\phi(n)} + n^{\phi(m)} \equiv 1 mod \ mn$?

Since the $gcd(m,n)=1$, by Euler's theorem $m^{\phi(n)} \equiv 1 mod \ n$ and $n^{\phi(n)} \equiv 1 mod \ m$. But $m^{\phi(n)} \equiv 0 \ mod \ m$ and $n^{\phi(n)} \equiv 0 \ mod \ n$. Therefore, $m^{\phi(n)} + n^{\phi(m)} \equiv (1+0) mod \ n \equiv 1 mod \ n$ and $m^{\phi(n)} + n^{\phi(m)} \equiv (1+0) mod \ m \equiv 1 mod \ m$.

Therefore, $m^{\phi(n)} + n^{\phi(m)} \equiv 1 mod \ mn$

2.)
a. Boss A and his set of friends B = {b1,b2,…, bn} collectively share a symmetric key $E_{AES-ABi}$
b. A encrypts each member of the set of keywords, K = {k1, k2, …, kn}, with $E_{AES-ABi}$ to obtain K' = {E(k1), E(k2),…, E(kn)}.
c. A encrypts each member of the set of friends, B = {b1,b2,…, bn}, with $E_{AES-ABi}$ to obtain B' = {E(b1), E(b2),…, E(bn)}.
d. To create the Bloom filter for K', A creates an array L of size q and r hash functions {h1, h2,…, hr | hi : K' ->{0,1,…, q-1}}, such that A initially sets L to 0, for any E(k) ∈ K', and then A sets L[hi(E(k))] = 1 for 1 ≤ i ≤ r.
e. To create the Bloom filter for B', A creates an array R of size q and s hash functions {h1, h2,…, hs | hi : B' ->{0,1,…, q-1}}, such that A initially sets R to 0, for any E(b) ∈ B', and then A sets R[hi(E(b))] = 1 for 1 ≤ i ≤ s .
f. A sends L, q hash functions, R and s hash functions to Secretary S.
g. A friend bi forwards a message, with set of encrypted keywords P = {E(k1) …, E(km)} and his/her encrypted information, E(bx), sent to S.
h. S will check to see if E(bx) ∈ B' by checking whether all locations of R[hi(E(bx))], for 1 ≤ i ≤ s, is set to 1. If this is true, S will check for the keyword or will discard the message if otherwise.

i. S will check if $E(kj) \in K'$, for $0 \leq j \leq m$, by checking whether all locations of $L[hi(E(kj))]$, for $1 \leq i \leq r$, is set to 1. If this is true, S will forward the message or will discard the message if otherwise.
j. A and S can also share a symmetric key, which is different from EAES-ABi, to encrypt communication if necessary.

3.) a. For each element in the set $A = \{a1, a2, \ldots an\}$, Alice computes two random numbers per bit of the element to obtain a set $R = \{\{\alpha0, \alpha1, \beta0, \beta1, \ldots\}_1, \{\alpha0, \alpha1, \beta0, \beta1, \ldots\}_2, \ldots, \{\alpha0, \alpha1, \beta0, \beta1, \ldots\}_n\}$.
b. For each element ai and based on the values of each bit in ai Alice selects the appropriate random numbers from R, and XORs them to generate a set of values $A' = \{x1, x2, x3 \ldots xn\}$ where $\alpha_{\{0,1\}} \oplus \beta_{\{0,1\}} \ldots = xi$ for all for $1 \leq i \leq n$.
c. Alice sends A' and R to Bob and Carlos.
d. For each element bi, in the set $B = \{b1, b2,, \ldots bn\}$ and based on the values of each bit in bi, Bob selects the appropriate random numbers from R, and XORs them to generate a set of values $B' = \{y1, y2, y3 \ldots yn\}$ where $\alpha_{\{0,1\}} \oplus \beta_{\{0,1\}} \ldots = yi$ for all for $1 \leq i \leq n$.
e. Bob compares B' and A' to find similar values to generate $A \cap B$
f. Bob sends $A \cap B$ to C
g. For each element, ci, in the set $C = \{c1, c2,, \ldots cn\}$ and based on the values of each bit in ci, Carlos selects the appropriate random numbers from R, and XORs them to generate a set of values $C' = \{z1, z2, z3 \ldots zn\}$ where $\alpha_{\{0,1\}} \oplus \beta_{\{0,1\}} \ldots = zi$ for all for $1 \leq i \leq n$.
h. Carlos compares C' to $A \cap B$ to find similar values to generate $A \cap B \cap C$.

4.) a. Assuming Alice has input $x = 001$ and Bob has input $y = 011$
b. Bob prepares to two random numbers per bit of $y = 011$. For *0*, α_0 and α_1 are created. For *1*, β_0 and β_1 are created. For *1*, γ_0 and γ_1 are created.
c. Bob sends α_0, α_1, β_0, β_1, γ_0 and γ_1 to Alice.
d. Based on the value each bit Bob has in $y = 011$, Bob selects the corresponding random number from each pair. For *0*, α_0 is selected; for *1*, β_1 is selected; and for *1*, γ_1 is selected.
e. Bob computes $C = \alpha_0 \oplus \beta_1 \oplus \gamma_1$ and sends C to Alice.
f. Based on the value each bit Alice has in $x = 001$, Alice selects the corresponding random number from each pair. For *0*, α_0 is selected; for *0*, β_0 is selected; and for *1*, γ_1 is selected.
g. Alice computes $D = \alpha_0 \oplus \beta_0 \oplus \gamma_1$
h. Alice compare C and D to determine whether $C = D$. If they are equal, comparison is completed.
i. If they are not equal, both Alice and Bob divide x and y into two parts.
j. Steps b to h are repeated on the most significant section of the x and y.
k. If they are equal, steps b to h are repeated on the least significant section of the x and y.
l. For either step j or k, if the bits are not equal, steps i to j are repeated for either section until only two bits are compared.
m. If they are not equal, Alice and Bob will expose their bits, the person with a value of 1 has the highest value.
n. If they are equal, Alice and Bob will move bitwise towards the right until unequal result is obtained, for which step m will be performed to see who has the highest value.