Number Theory & Cryptography

Assignment 2

Dear students, Please implement the questions given to you, demonstrate it and present it.

Submission Date: On or before second Internal examination.

Group 1: (AISHA NAMA ANTHOORATHODI, AKSHAYA M K, ALINA GEORGE)

Implement pollard-rho method and factorize a large integer n using different functions and compare the number iterations it takes for each.

Group 2: (AMAL MEHABIN P, ANJANA SANKAR K, ANUJITH P P)

Implement Continued Fraction method for factorization.

Group 3: (ASWIN P M, JEEVANDAS M S, JOSEPH VARGHESE)

a) Implement Diffie-Hellman key exchange method.

b) The prime 12347 has 2 as a primitive root. Suppose I tell you that $2^x \equiv 8938 \pmod{12347}$ and $2^y \equiv 9620 \pmod{12347}$, but I don't tell you x and y. Is $2^{xy} \equiv 7538 \pmod{12347}$? Is $2^{xy} \equiv 7557 \pmod{12347}$?
The Decisional Diffie–Hellman Problem asks the following question: Given g, g^a, g^b, and h, is $g^{ab} \equiv h \pmod{p}$? It is not known whether this can be solved without first solving the Computational Diffie–Hellman Problem. (Recall that this asks you, given g, g^a, and g^b, to compute g^{ab}.)

Group 4: (KARTHIK C V, KRISHNA AJITH, MAJIDA NASRIN M P)

a) For RSA, let p = 167 and q = 251, so n = 41917. Let e = 3. Encrypt ban = 20114, bat = 20120, and bay = 20125. Can you tell from the ciphertexts that only one letter has been changed in the plaintexts? (In a good cryptosystem, a small change in the plaintext makes a large change in the ciphertext.)

b) Find the decryption exponent d.

c) Bob tries to send you the ciphertext c = 27120, but there is a transmission error and you receive 27121. Do you obtain anything close to the intended message?

Group 5: (MARIYA JYOTHY, MUHANNAD MOHAMMED ALI, MUHSINA BEEGUM)

Implement ElGamal cryptosystem.

Group 6: (NANDAKISHORE V J, NIDAL NAAZ LUCKMAN, RABEAH BASHEER)

Implement Knapsack Cryptosystem.

Group 7: (RISHAN P N, SNEHAL P, THEJUS S)

Implement RSA signature scheme.