COMP3355—Lab 1 Report

Shaheer Ziya (3035946760)

Task 1

RSA Encryption

Recall that in RSA we generate a public key (e, N) and a private key (d, N), where ‘e’ and ‘d’ are the encryption and decryption exponents respectively while ’N’ is the product of the two (large) primes picked initially.

To encrypt a message using RSA, we begin by encoding our message into a numerical value, then split the data into blocks of fixed size strictly less than N.

For each block M_i, we compute $C_i = M_i^e \pmod N$, where C_i is the encrypted cipher for each block. Although we can encrypt using any key, often we use the encryption exponent from the private key to encrypt messages.

Decryption with private key

Likewise, to decrypt the message, we take the encrypted data, split it into the same fixed size chunks as at the time of encryption (often in practice being 1024, 2048 or 4096 bits), and then perform the computation, $M_i = C_i^d \pmod N$, where C_i is the number represented by the fixed block of data and ‘d’ is the decryption exponent from the private key. We can then de-encode the chunks M_i to retrieve the original message.

Task 2

Small Exponent & Short Message Attack

Recall the the cipher text, C, is $C = M^e \pmod{N}$. Since $e = 3$ and $M << N$, we know that because $M = (C - kN)^{\frac{1}{3}}$, where k is an integer, must have a limited number of solutions that we can verify through trial and error.

Attack Prevention

Besides increasing the length of the exponent, we can consider padding the short message to make the encryption less vulnerable.

Task 3

Ps & Qs Attack

The basic idea behind Ps & Qs attack is that if multiple users have moduli that share common primes, then a malicious actor can reverse engineer their private key. RSA's security relies on the fact that factoring large numbers into primes is incredibly slow, however computing the GCD of certain numbers is much more efficient, which comes into play when the moduli have shared prime factors.

Although the provided reference details a distributed approach to the problem we make the simplifying assumption that say two users have moduli (N_1, N_2) that share a prime factor for

the sake of explanation. If $N_1 = P \cdot Q_1$ and $N_2 = P \cdot Q_2$, where P, Q_1, Q_2 are prime numbers, then we can compute their GCD (which is exactly P) to obtain Q_1 and Q_2. This allows us to quickly compute the decryption exponent from the definition of RSA Key Generation Algorithm, namely, $d = e^{-1} \pmod{(p-1)(q-1)}$.

Attack Prevention

The problem arises in part because of low entropy in the random number generator in computing systems which lead to there being common primes in the moduli of the public keys. A solution could be to use larger primes with more secure random number generators so that the likelihood of this scenario occurring is minimised. We can also consider adding a random padding at the end of the message so that we cannot deterministically determine the message.

Task 4

Håstad's Broadcast Attack

The working principle in the broadcast attack is that the same message encrypted with different public keys can be deciphered if certain conditions are met. In particular if the the encryption exponent is three than having only three messages (encrypted with different public keys) can be sufficient for us to decrypt the message. We can compute the coefficient C which is equivalent to the message cubed M^3, modulo $N_1 N_2 N_3$ using the Chinese Remainder Theorem. Since the encryption exponent is three, both of these must be identical and so computing the cube root gives us the exact message (after rounding to the closest integer).

Note that we need to assume that all the moduli in the public keys are pairwise co-prime to apply the CRT, in case they are not we can decode the message using an approach shown earlier in the homework.

Two Cipertext instead of Three

In the case when there are only two ciphers instead of three, if the moduli are co-prime, we are unable to satisfy the requirements for applying the CRT since we can not uniquely determine the value of $M^3 \pmod{N_1 N_2}$.