Cryptography
ECE 5632
Sheet 6

Spring 2023

Problem 1

In an RSA cryptosystem, let the two secret primes be $p = 59$ and $q = 53$. Satisfy the following:

(a) Compute $\phi(n)$.

(b) Pick a suitable public key (e) from the list of numbers: $16, 18, 36, 42, 45, 87$.

(c) Compute the private key (d).

(d) For a message $x = 731$, compute the RSA encryption of x.

(e) Decrypt the RSA ciphertext$y = 16$.

Problem 2

Given the list of small primes: [2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97]

(a) What is the factorization of $n = pq$ if p and q are primes and $n = 1763$.

(b) Compute the Euler function $\phi(n)$ for n.

Problem 3

Consider an RSA cryptosystem where the RSA modulus $n = 77$. Compute the following:

(a) $\phi(n)$.

(b) If the public exponent e is chosen to be 7, what is the private exponent d?

(c) Encrypt $m = (01101)_b$ using (e, n) as the public key.

(d) If the intercepted ciphertext is $(10101)_b$ what is the corresponding plaintext message x?

Problem 4

Perform encryption and decryption using the RSA algorithm for the following:

(a) $p = 3; q = 11, e = 7; x = 5$

(b) $p = 5; q = 11, e = 3; x = 9$

Problem 5

In an RSA system, the public key of a given user is $e = 31$, $n = 3599$. What is the private key of this user? Hint: First use trial-and-error to determine$p$ and q; then use the extended Euclidean algorithm to find the multiplicative inverse of 31 modulo $\phi(n)$.

Problem 6

In an RSA public key encryption, you intercept the ciphertext$y = 10$ sent to a user whose public exponent is $e = 5$ and RSA modulus $n = 35$. Can you find x through cryptanalysis?

Problem 7

For each of the multiplicative groups $Z_7^*, Z_{13}^*, Z_{53}^*$, what are the possible element orders?

Problem 8

Compute the two public keys and the common key for the DHKE scheme with the parameters $p = 467, \alpha = 2$, and

(a) $a = 3, b = 5$

(b) $a = 400, b = 134$

(c) $a = 228, b = 57$

In all cases, perform the computation of the common key for Alice and for Bob. This is also a check of your results.

Problem 9

Users Alice and Bob use the Diffie-Hellman key exchange technique with a common prime $p = 71$ and a primitive root$\alpha = 7$.

(a) If Alice has private key $a = 5$, what is Alice's public key$A$?

(b) If Bob has private key b, what is Bob's public key B?

(c) What is the shared secret key K_{AB}?

Problem 10

Consider a Diffie-Hellman scheme with a common prime $p = 11$ and a primitive root $\alpha = 2$.

(a) Show that 2 is a primitive root of 11.

(b) If Alice has public key $A = 9$, what is Alice's private key a?

(c) If Bob has public key $B = 3$, what is the secret key K_{AB} shared with Alice?

Problem 11

Describe the Diffie-Helman key exchange (DHKE) protocol. Explain the man-in-the-middle attack against DHKE.