CS 3873: Net-Centric Computing

Assignment 5: Network Security and Link Layer

Student Name: _Adrian Freeman_ Student Number: _3661616__

[Mandatory] Declaration: “I warrant that this is my own work.”

Signed by _Adrian Freeman_

(You can type in your name as your signature.)

From the UNB Undergraduate Calendar, available at the website:
http://www.unb.ca/academics/calendar/undergraduate/current/regulations/universitywideacademicregulations/viii-academicoffences/index.html.

“Plagiarism includes:

1. quoting verbatim or almost verbatim from any source, regardless of format, without acknowledgement;
2. adopting someone else's line of thought, argument, arrangement, or supporting evidence (such as, statistics, bibliographies, etc.) without indicating such dependence;
3. submitting someone else's work, in whatever form (essay, film, workbook, artwork, computer materials, etc.) without acknowledgement;
4. knowingly representing as one's own work any idea of another.”

Penalties for plagiarism and other academic offences can be found at the above website.

1) How big is the MAC address space? The IPv4 address space? The IPv6 address space?
    - MAC Address Space: 48 Bits, so 2^{48} addresses ~ 281 Trillion
    - IPv4 Address Space: 32 Bits, so 2^{32} addresses ~ 4.3 Billion
    - IPv6 Address Space: 128 Bits, so 2^{128} addresses ~ 3.4×10^{38}

2) Consider RSA with p = 17 and q = 13.
    a) What are n and z?
        - n = p * q
            - = 17 * 13
            - = 221
        - z = (p–1) * (q-1)
            - = 16 * 12
            - = 192
    b) Let e be 77. Find d such that ed = 1 (mod z) and d < z.

        p = 17, q = 13, n = 221, z = 192, e = 77

        e*d = k*z + 1

        77d = 1 * 192 + 1 = 193, 193 / 77 = 2.506

        77d = 2 * 192 + 1 = 385

        d = 385 / 77 = 5
    c) Encrypt the message m = 4 using the public key (n, e). Let c denote the corresponding cipher text.

        Hint: To simplify the calculations, use the fact: [(a mod n) • (b mod n)] mod n = (a · b) mod n

        $c = m^e \bmod n$

        $3^{77} \bmod 221$

        $3^{77} \bmod 221 = (3^{64} * 3^8 * 3^4 + 3^1) \bmod 221$

        $= (((((3^{64} * 3^8) \bmod 221) * 3^4) \bmod 221) * 3^1) \bmod 221$

        $3^1 \bmod 221 = 3 \bmod 221 = 3$

        $3^2 \bmod 221 = 9 \bmod 221 = 9$

        $3^4 \bmod 221 = (3^2)^2 \bmod 221 = 9^2 \bmod 221 = 81 \bmod 221 = 81$

        $3^8 \bmod 221 = (3^4)^2 \bmod 221 = 81^2 \bmod 221 = 6561 \bmod 221 = 152$

$3^{16} \bmod 221 = (3^8)^2 \bmod 221 = 152^2 \bmod 221 = 23104 \bmod 221 = 120$

$3^{32} \bmod 221 = (3^{16})^2 \bmod 221 = 120^2 \bmod 221 = 14400 \bmod 221 = 35$

$3^{64} \bmod 221 = (3^{32})^2 \bmod 221 = 35^2 \bmod 221 = 1225 \bmod 221 = 120$

$3^{77} \bmod 221 = (((((3^{64} * 3^8) \bmod 221) * 3^4) \bmod 221) * 3^1) \bmod 221$

$(3^{64} * 3^8) \bmod 221 = (120 * 152) \bmod 221 = 18240 \bmod 221 = 118$

$(118 * 3^4) \bmod 221 = (118 * 81) \bmod 221 = 9558 \bmod 221 = 55$

$(55 * 3^1) \bmod 221 = (55 * 3) \bmod 221 = 165 \bmod 221 = 165$

$3^{77} \bmod 221 = 165$

c = 165

3)

a) Suppose that the receiver receives a two-dimensional even parity matrix as follows. Is there an error in the matrix? If yes, can you tell which bit(s) are wrong?

The parity matrix has an error in Column 4 Row 1 and Column 4 Row 3, as both are 0s and should be 1s

1	0	0	0
0	1	0	1
0	1	0	0
1	0	0	1

b) Now suppose the received parity matrix is the following. Suppose you know there is at most one bit error, can you correct the error?

The parity matrix has an error in Column 2 Row 3.

1	0	1	0
0	0	1	1
1	1	1	0
0	0	1	1

1	0	1	0
0	0	1	1
1	0	1	0
0	0	1	1

4) Suppose Alice wants to send an e-mail to Bob. Bob has a public-private key pair (E_B, D_B), and Alice has Bob's certificate that include Bob's public key E_B. But Alice does not have a public-private key pair. Alice and Bob (and the entire world) share the same hash function H(.).

   a) In this situation, is it possible to design a scheme so that Bob can check the integrity of the message received from Alice? If so, how should Alice send the message and how should Bob process the received message from Alice.

      Alice computes hash of message M, (H(M)), using H(.)

      Alice sends both M and H(M) to Bob.

      Bob computes hash of received message M, (H'(M)), using H(.)

      Compare H'(M) and H(M), if they match, the message has retained its integrity. Otherwise it has been tampered with.

   b) Is it possible to design a scheme that provides confidentiality for sending the message from Alice to Bob? If so, how should Alice send the message and how should Bob process the received message from Alice.

      Alice encrypts message M using Bob's public key E_B, $C = E_B(M)$

      Alice sends C to Bob

      Bob decrypts C using D_B and gets M

   c) Is it possible to design a scheme so that Bob can verify that Alice created the message? If so, how should Alice send the message and how should Bob process the received message from Alice?

      No, Alice needs a public-private key pair to sign her messages. After she sends the message, Bob can verify the signature using Alice's public key.

5) Consider the generator G = 10111 for CRC and the following D (the data bits). What is the value of R (the check bits) for each D? Show your calculation process.

a) 1010101110

10111/10101011100000

XOR10111

00010011

XOR10111

0010010

XOR10111

0010100

XOR10111

000**1100**

R = 1100 or 12

b) 1001010101

10111/10010101010000

XOR10111

0010110

XOR10111

000011010

XOR10111

011010

XOR10111

011010

XOR10111

011010

XOR10111

0**1101**

R = 1101 or 13

c) 0101101110

10111/01011011100000

XOR10111

11100

XOR10111

010110

XOR10111

000011110

XOR10111

010010

XOR10111

0010100

XOR10111

000**110**

R = 110 or 6

d) 1010100000

10111/10101000000000

XOR10111

00010000

XOR10111

0011100

XOR10111

010110

XOR10111

0000**1000**

R = 1000 or 8