FINAL, MATH 587/CSCE 557 - MAY 2, 2007

Answer any FIVE of the six questions. Show your working. Full credit will not be given for the answer without any justification. Make sure you answer each part of each question. Do not write essays! Concise, "to-the-point" answers are favored.

1. (a) How many affine ciphers are there?

Answer: $e(x) = ax + b \pmod{26}$ where b is any element of $\mathbf{Z}_{26}$ and a any element of $\mathbf{Z}_{26}^*$, which has 12 elements. So $26 * 12 = 312$.

(b) State the three kinds of attacks on cryptosystems.

Answer: chosen-plaintext, known-plaintext, ciphertext-only.

(c) Suppose JFFGJFDMGFSJHYQHTAGHQGAFDCCFP is the ciphertext produced by an affine cipher applied to an English message. Find the encryption and decryption keys and the plaintext, explaining your method. What kind of attack is this?

Answer: The most frequent letter is F and second most frequent G. Say F decrypts to E and G to T. If $d(y) = cy + d \pmod{26}$, then $4 = 5c + d, 19 = 6c + d$. Subtracting, $c = 15$ and then $d = 4 - 5 * 15 = -71 = 7$. Using $d(y) = 15y + 7 \pmod{26}$ sends A,C,D,H,J,M,P,Q,S,T,Y to H,L,A,I,M,F,Y,N,R,G,D and gives message: Meet me after midnight in the alley. If $x = 15y + 7$, then $e(x) = y = (x - 7)/15 = 7(x - 7) = 7x - 49 = 7x + 3 \pmod{26}$. A ciphertext-only attack.

2. (a) Define the index of coincidence of a message.

Answer: It is the proportion of pairs taken from the message that match.

(b) Say an English phrase yields the ciphertext RFCRCYAFCP. Compute its index of coincidence. Why does it suggest that a monoalphabetic cipher was used?

Answer: The index of coincidence is $(n_A(n_A - 1) + ... + n_Z(n_Z - 1))/(n(n - 1))$ where n_A is the number of A's in the message, n_B the number of B's, etc. and n the length of the message. $n_C = 3, n_F = 2, n_R = 2$ and all others are ≤ 1, so the IC is $(3 * 2 + 2 * 1 + 2 * 1)/(10 * 9) = 1/9 = 0.111$. This is so large that it's likely to be created by a monoalphabetic cipher.

(c) Say a Vigenere cipher was used. Find the plaintext, explaining your method.

Answer: A monoalphabetic Vigenere is a shift cipher. Suppose the most frequent letter C decrypts to E, a shift of 2. Then the plaintext is The Teacher.

3. (a) A linear feedback shift register produces the bit stream 100011110... Show that it cannot be a 3-cell register, but that it could be a 4-cell register. Find the recurrence relation (rule) of this 4-cell register and use it to find the first 20 bits and the period.

Answer: A 3-cell register cannot have 3 consecutive zeros. Say it comes from the 4-cell register $x_{i+4} = c_0x_i + c_1x_{i+1} + c_2x_{i+2} + c_3x_{i+3}$. Plugging in $i = 0, 1, 2, 3$ gives equations $\pmod 2$: $1 = c_0, 1 = c_3, 1 = c_2 + c_3, 1 = c_1 + c_2 + c_3$, so $c_0 = 1, c_1 = 0, c_2 = 0, c_3 = 1$, i.e. the rule is $x_{i+4} = x_i + x_{i+3}$. This correctly produces $x_8 = 0$ so the bit stream could come from this 4-cell register. The first 20 bits are: 10001111010110010001. The period is 15.

(b) If this LFSR produces ciphertext 10111011110001010111, find the plaintext.

Answer: Adding the ciphertext to the key produces 00110100100111000110.

4. (a) Suppose that a block cipher is defined as follows. Encrypt bit strings of length 6 by mapping $x_1, x_2, x_3, x_4, x_5, x_6$ to $x_4, x_5, x_6, x_1+x_5+x_6, x_2+x_4+x_6, x_3+x_4+x_5$. What is this kind of cipher called? Encrypt 100111. Decrypt 100111.

Answer: A Feistel cipher. Encrypting, we get 111100. To decrypt, setting $x_4 = 1, x_5 = 0, x_6 = 0, x_1 + x_5 + x_6 = 1, x_2 + x_4 + x_6 = 1, x_3 + x_4 + x_5 = 1$, we solve to get $x_4 = 1, x_5 = 0, x_6 = 0, x_1 = 1, x_2 = 0, x_3 = 0$, so decrypts to 100100.

(b) If $y_1, y_2, y_3, y_4, y_5, y_6$ is the ciphertext, what is the corresponding plaintext?

Answer: Setting $x_4 = y_1, x_5 = y_2, x_6 = y_3, x_1 + x_5 + x_6 = y_4, x_2 + x_4 + x_6 = y_5, x_3+x_4+x_5 = y_6$, we solve to get $x_4 = y_1, x_5 = y_2, x_6 = y_3, x_1 = y_4+y_2+y_3, x_2 = y_5 + y_1 + y_3, x_3 = y_6 + y_1 + y_2$, so decrypts to $y_2 + y_3 + y_4, y_1 + y_3 + y_5, y_1 + y_2 + y_6, y_1, y_2, y_3$.

(c) Describe in two to three sentences the main points about how DES works.

Answer: DES is a block cipher with blocks of length 64 and a key of length 56, consisting of 16 Feistel rounds combined with various permutations to mix up the bits. A key schedule produces the 16 48-bit subkeys from the main key.

5. (a) Suppose Bob has RSA public key $N = 15, e = 3$. By factoring N, find his private decryption exponent d. Suppose Alice wants to send message $x = 3$ to Bob - what ciphertext y should she send? Check that decrypting y indeed produces x.

Answer: $N = 3{*}5$ so $de \pmod 8 = 1$. Since $e = 3$, $d = 3$. $y = 3^3 \pmod{15} = 12$. To decrypt, Bob computes $12^3 \pmod{15}$. The easiest way to do this is as $(-3)^3 \pmod{15} = -3^3 \pmod{15} = -12 \pmod{15} = 3$. So it checks.

(b) Suppose Bob has RSA public key (N, e) (with more realistic values than in part (a)). Alice wants to send Bob her credit card number x and Oscar wants to steal it. Oscar sets up a webpage that looks like Bob's with Oscar's own RSA public key (N', e') on which Alice submits her credit card number encrypted with Oscar's key. Show that Oscar successfully steals x. To ensure that Bob and Alice suspect nothing, what should Oscar send to Bob and Alice?

Answer: Alice sends Oscar $y = x^{e'} \pmod{N'}$ and Oscar simply computes $y^{d'} \pmod{N'} = x$. He should then send Bob $x^e \pmod N$ (Oscar now impersonating Alice) and if Bob sends a reply confirming receipt, just forward it to Alice.

6. (a) Suppose Alice and Bob perform Diffie-Hellman key exchange with prime $p = 257 = 2^8 + 1$. This produces a shared key $k = g^{ab} \pmod p$ where a and b are Alice's and Bob's respective secret exponents. Produce a scheme whereby k is represented by a byte (i.e. bit string of length 8). Using this scheme, what byte is their key if $g = 2, a = 3$ and $b = 5$?

Answer: k will be an integer between 1 and 256 so turn this into binary (if $k = 256$, then use the all zero byte). $2^{15} \pmod{257} = 2^8 * 2^7 \pmod{257} = -128 \pmod{257} = 129$. In binary, this is 10000001.

(b) Alice and Bob agree on $g = 2$. Show that if ab is divisible by 8, then k is 1 or 256. For randomly chosen a, b, how often does this happen? [Hint: consider possible $a \pmod 8$ and $b \pmod 8$.] Why does this mean that this choice of p, g is bad?

Answer: If $ab = 8r$, then $2^{ab} \pmod{257} = 2^{8r} \pmod{257} = (-1)^r \pmod{257}$. If r is even, you get 1. If r is odd, you get 256. Of the 64 possibilities for $a \pmod 8), b \pmod 8$, 20 give $ab \pmod 8 = 0$. So $20/64 = 5/16$ of the time. Almost a third of the time the key is one of only two possibilities - this is bad.