Massachusetts Institute of Technology
6.857: Network and Computer Security
Professor Ronald L. Rivest

Handout 5
September 24, 1998

Problem Set 2

This problem set is due on *Thursday, October 1* at the end of class. Please keep your answers *short*. Mark the top of your sheets with your names, 6.857, the problem number, and the date. You MUST work in groups of 3 to 4 people. You do not need to work in the same group as you did for the previous homework. Late solutions will not be accepted.

Problem 2-1. Cryptanalysis of a Block Cipher

Here is a proposed block cipher that has 64-bit message and ciphertext blocks. The point of this problem is to illustrate the power of chosen plaintext attacks.

Let the bit positions of the message and ciphertext blocks be labelled from 0 starting with the low-order bit.

The secret key shared between the sender and receiver consists of three parts:

1. An initial permutation $\pi : \{0, ..., 63\} \longrightarrow \{0, ..., 63\}$.
2. A set of eight S-boxes $(S_0, ..., S_7)$. Each S-box takes eight input bits and returns eight output-bits. That is, their domain and range are $\{0, 1\}^8$. Each S-box is one-to-one and onto. (This last is required so that you can decode a ciphertext.)
3. A final permuation $\mu : \{0, ..., 63\} \longrightarrow \{0, ..., 63\}$.

The cipher works in the following steps. Suppose the input message is a bit vector $a[0..63]$.

1. Create the intermediate vector $b[0..63]$ by applying permutation π to the input vector a:

$$\text{for } i = 0, .., 63 : b[\pi(i)] = a[i]$$

2. Create the intermediate vector $c[0..63]$ by applying the S-boxes to b:

$$\text{for } i = 0, ..., 7 : c[i * 8..i * 8 + 7] = S_i(b[i * 8..i * 8 + 7])$$

3. Create the final ciphertext $d[0..63]$ by applying the permutation μ to c:

$$\text{for } i = 0, ..., 63 : d[\mu[i]] = c[i]$$

(a) Argue that this block cipher can be easily broken with a chosen plaintext / chosen ciphertext attack. (You choose the plaintext, and get to see the resulting ciphertext, or you supply the ciphertext and get to see the resulting plaintext.)

(b) How many chosen plaintexts are needed to break the cipher? (Your attack procedure need not come up with the actual values for the permutations and S-boxes, but may come up with "equivalent" ones that yield the same encryption operation.)

(Breaking this cipher when you only get to observe, instead of choose, the plaintext or ciphertext, seems much harder. With more rounds of alternating substitution and permutation, even chosen plaintext and chosen ciphertext attacks may be inadequate to break the cipher efficiently.)

Problem 2-2. Cascade Ciphers

Let E_1 and E_2 be two encryption algorithms, with corresponding decryption algorithms D_1 and D_2. Define the composed encryption scheme

$$E_3((K1, K2), M) = E_2(K2, E_1(K1, M))$$

obtained by first applying $E1$ to the message M using key $K1$, and then applying $E2$ to the result, using key $K2$. This is sometimes called a *cascade cipher*, or *double encryption* (with different schemes). The encryption key for E_3 is the ordered pair of keys $(K1, K2)$ for the two sub-encryption schemes E_1, E_2.

Suppose that we are interested in the security of these scheme against chosen plaintext and chosen ciphertext attack (the adversary can do either), where the adversary's goal is to find the unknown key.

(a) Argue carefully that *when the keys $K1$ and $K2$ are chosen independently*, the scheme E_3 is at least as secure as E_1 and at least as secure as E_2. (Two separate, but similar, arguments required. Show how to reduce an attack on E_1 or E_2 to an attack on E_3.)

(b) Give an example to show that the claim of the previous part may be false when the keys are not chosen independently.

(c) Give similar arguments for the above two parts for stream ciphers instead of block ciphers. Here the pad generated by E_3 is defined to be the xor of the pads generated by E_1 and E_2. The adversary is again trying to find the unknown key, using known plaintext/ciphertext pairs.

Problem 2-3. Finite Fields

Finite fields of size q exist whenever q is a prime or a prime power. These are sometimes denoted as $GF(q)$ or $GF(p^k)$ if $q = p^k$ where p is prime and $k \geq 1$. When $q = p$ is just a prime, then $GF(p)$ is just arithmetic modulo p. When $q = p^k$ for $k > 1$, then we can define $GF(q)$ by using univariate polynomials of degree at most $k - 1$ with coefficients chosen modulo p. Polynomials with degree larger than $k - 1$ are reduced by taking them modulo a fixed irreducible polynomial $f(x)$ of degree k. (For example, x^5 modulo $x^3 + x + 1$ (with coefficients modulo 2) is just $x^2(x + 1) = x^2 + x + 1$ since $x = -x$ modulo 2 and $x^3 = x + 1$ modulo $x^3 + x + 1$.) Irreducible, or "prime", polynomials, have no smaller polynomial factors.

(a) Give the complete addition and multiplication tables for $GF(2^3)$, where the irreducible polynomial used is $x^3 + x + 1$. Give the additive inverse of each element. Give the multiplicative inverse of each nonzero element. This field has 8 elements: $0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1$. You can represent their coefficients compactly if you wish in the natural manner: $(000), (001), (010), (011), (100), (101), (110), (111)$ for the above list.

(b) Determine the multiplicative order of each nonzero element. (An element r has multiplicative order t if t is the least positive integer such that $r^t = 1$.) List any generators (elements of order 7 whose powers generate all nonzero elements).

(c) Argue that $(a + b)^p = a^p + b^p$ in $\mathrm{GF}(p^k)$. (Use the binomial theorem to expand $(a + b)^p$.)