0368.3049.01 Introduction to Modern Cryptography Fall 2001

Assignment #1

This assignment contains 5 "dry" problems and 2 "wet" ones. Efficient solutions are always sought, but a solution that works inefficiently is better than none. The answers to the the "wet" problems should be given as the output of an XMAPLE session.

Problem 1 Let p be a 128-bit prime and let Z_p be the set of integers $\{0, \ldots, p-1\}$. Consider the following encryption scheme. The secret key is a pair of integers $a, b \in Z_p$ where $a \neq 0$. An encryption of a message $M \in Z_p$ is defined as:

$$E_{a,b}(M) = aM + b \bmod p$$

a Show that when E is used to encrypt a *single* message $M \in Z_p$, the system is a perfect cipher. (For a definition, refer to notes from the first lecture.)

b Show that when E is used to encrypt *two* messages $M_1, M_2 \in Z_p$, the system is *not* a perfect cipher.
Hint: Consider the case $M_1 = M_2$.

c Show that a known plaintext attack with just two pairs of plaintext/ciphertext $C_i = E_{a,b}(M_i)$ $(i = 1, 2)$ can recover the secret key a, b with high probability.

Problem 2 The following is a special case of a permutation cipher: Let m, n be positive integers. Partition the plaintext to segments of nm letters each. Write down each plaintext segment by *rows* in an n-by-m matrix. The ciphertext is created by going over the *columns* of the matrix. For example, if $n = 3$, $m = 4$ the plaintext "cryptography" will lead to the matrix and

c	r	y	p
t	o	g	r
a	p	h	y

the ciphertext will be "ctaropyghpry".

a. Decipher the ciphertext (generated in the abovementioned way, not necessarily with the same m and n) "myamraruyiqtenctorahroywdsoyeouarrgdernogw".

b. Describe an effective method for deciphering long enough ciphertexts, encrypted by applying a regular substitution cipher first, followed by a permutation cipher as above. Limit your answer to no more than 8 lines.

Problem 3 The following two keys enhancements to DES were proposed in order to increase the complexity of finding the keys by exhaustive search.

$$DESV_{k,k_1}(M) = DES_k(M) \oplus k_1,$$
$$DESW_{k,k_1}(M) = DES_k(M \oplus k_1)$$

The keys lengths is $|k| = 56$ and $|k_1| = 64$ (k_1 is the same length as the block length). Show that both these proposals do not increase the complexity of breaking the cryptosystem using brute-force key search. That is, show how to break these schemes using on the order of 2^{56} DES encryptions/decryptions. You may assume that you have a moderate number of plaintext-ciphertext pairs, $C_i = DESV/W_{k,k_1}(M_i)$.

Problem 4 In lecture 2 we described a *meet in the middle* attack against *double* DES. The attack required 2^{56} decryptions, 2^{56} encryptions and storage for 2^{56} messages (the decryptions of the ciphertext under all possible keys), 64 bits each. The attack used a small plaintext/ciphertext pairs: M_i and $C_i = DES_{k_2}(DES_{k_1}(M_i))$.

You were hired to perform the same task, only your employer, hurt by the recent market trends, has supplied you with a machine capable of storing only 2^{40} words of 64 bits each. How many encryption and decryption operations do you need in order to recover the secret key k_1, k_2 with high probability. Does the number of required plaintext/ciphertext pairs increase?

Problem 5 RTAU (an Internet Music Station) wishes to broadcast streamed music to its subscribers. Non-subscribers should not be able to listen in. When a person subscrIbes she is given a software player with a number of secret keys embedded in it. RTAU encrypts the broadcast using a 128-bit AES key K. The secret keys in each legitimate player can be used to derive K and enable legitimate subscribers to tune in. When a subscriber cancels her subscription, RTAU will encrypt future broadcasts using a different key K'. All legal subscribers should be able to derive K' , while the canceled subscriber should not.

a. Suppose the total number of potential subscribers is less than $n = 10^5$. Let $R_1, R_2, \ldots, R_n$ be n random independent values, 128 bits each . The

player shipped to subscriber number u contains all the R_i's except for R_u (*i.e.* each player contains 99999 keys). Let S be the set of currently subscribed users. Show that RTAU can construct a key K, used to encrypt the broadcast, so that every subscriber in S can derive K (from the R_i's in her player), while any single subscriber outside of S cannot derive K. You may assume that the set S is known to everyone (e.g. it is a plain part of the broadcast) . Briefly explain why your construction satisfies the required properties.

b. Is your construction in part (a) collusion resistant? That is, can two canceled subscribers combine the secrets embedded in their player to build a new operational player?
Remark: Much better solutions to this problem exist.

Problem 6 In this problem we will become familiar with finite fields $GF(p^k)$ where $k > 1$. Specifically, we will look at the field $GF(2^4)$.

Find an irreducible polynomial $f(x)$ of degree 4 over the base field of characteristic 2, Z_2. Implement the field $GF(2^4)$ in MAPLE using the two statements

```
G16:=GF(2,4,f(x));
a := G16[ConvertIn](x);
```

Once this is done, write a small loop which prints out all the primitive elements (multiplicative generators) in $GF(2^4)$. How many are there? The situation here is quite different than that of $GF(2^5)$. Briefly explain why. (`ConvertOut` is a canonical representation of field elements, with higher degree momonials to the left.)

Problem 7 Pick *at random* a 5 digit number a and a 6 digit number b that are relatively prime. Using just MAPLE's `mod`, run Euclid gcd algorithm on a and b. How many steps did it take? Now run the extended gcd algorithm and compute the multiplicative inverse of a in Z_b.