MATC16 Cryptography and Coding Theory
Gábor Pete
University of Toronto Scarborough
gpete at utsc dot utoronto dot ca

Homework Assignment 2 (Due March 3 Thu)

Don't just give the answers, but indicate clearly the arguments you have followed.

Problem 1. A common way to store passwords on a computer is to use DES with the password as the key to encrypt a fixed plaintext (usually $00\cdots 0$). The ciphertext is then stored in the file. When you log in, the procedure is repeated, and the ciphertexts are compared. Why is this method more secure than the similar-sounding method of using the password as the plaintext and using a fixed known key (for example, $00\cdots 0$)? **(1 pt)**

Problem 2. Viewing the affine cipher as a double encryption, first multiplication by α, then shift by β, describe how a meet-in-the middle attack on a known plaintext-ciphertext pair works. Is this faster here than brute force key search? **(2 pts)**

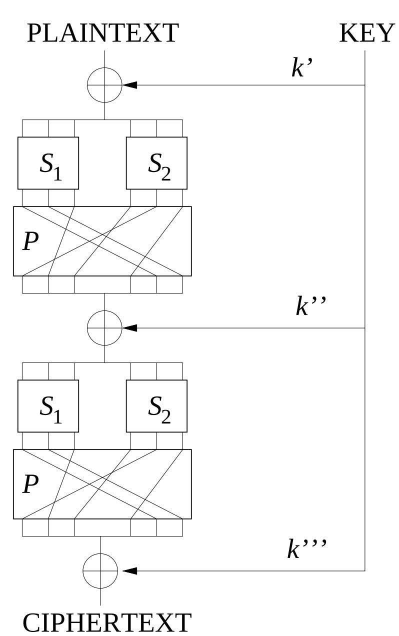
Problem 3. Consider the Cipher Block Chaining (CBC) mode of operation for some block cipher (say, AES), applied to the plaintext P with blocks $P_1, P_2, \ldots, P_n$. If an error occurs in the transmission of a ciphertext block C_j from Alice to Bob, but all other blocks are transmitted correctly, how many blocks will be affected at decryption? **(2 pts)**

Problem 4. Consider the substitution-permutation network depicted on the right, encrypting 6-bit plaintexts. The P-box is shown on the picture; the S-boxes act by multiplying row vectors from the right by the following matrices:

$$S_1 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \text{ and } S_2 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

A 6-bit key $\underline{k} = k_1 k_2 \ldots k_6$ gives the three rounds keys $\underline{k}' = k_1 k_3 k_5 k_2 k_4 k_6$, $\underline{k}'' = k_5 k_6 k_3 k_4 k_1 k_2$, and $\underline{k}''' = k_6 k_1 k_4 k_3 k_2 k_5$.

Choose a pair of random 6-bit sequences, $\underline{x}$ and $\underline{y}$; say, flip coins or take your student ID (mod 64) and rewrite the result in binary. Assume that the plaintext $\underline{x}$ gets encrypted into the ciphertext $\underline{y}$. Find the key! (Hint: each transformation here is linear, acting on vectors of length 6.) **(4 pts)**



Problem 5.

(a) Show that if p is a prime and $1 \leq k \leq p-1$, then $p \,\Big|\, \binom{p}{k} = \frac{p!}{k!\,(p-k)!}$ **(1 pt)**

(b) Using part (a), show that if p is a prime, then $x^p + 1$ is a reducible polynomial in $\mathbb{Z}_p[x]$. (Hint: consider first the $p = 2$ case.) **(1 pt)**

(c) How many elements does $\mathbb{Z}_3[x] \pmod{x^3 + 1}$ have? Show that with the usual $+$ and $\cdot$ operations it is not a field. **(2 pts)**

(d) Show that the polynomial $x^2 + 1$ is irreducible in $\mathbb{Z}_3[x]$. **(1 pts)**

(e) Take your student ID, $a_8 a_7 \ldots a_0$. What is the polynomial $a_8 x^8 + a_7 x^7 + \cdots + a_1 x + a_0$ in the finite field $\mathbb{Z}_3[x]/(x^2 + 1)$? What is its multiplicative inverse? **(3 pts)**

Problem 6. What is the last digit of 7^{7^7} (i.e., 7 to the power 7^7)? **(3 pts)**

Problem 7. Consider $n = 17 \cdot 31 = 527$. How many square roots can a given number have (mod n)? Find an example for each possibility. **(4 pts)**

(Max possible score: **24 pts**)