Name:

Topic in Mathematics (Math 4613)
Cryptography
Practice Final Exam

Professor Paul Bailey
December 12, 2007

The examination contains eight problems worth fifteen points each. Four of the problems are mathematical, and four of the problems involve programming to decrypt given files.

You may visit `www.saumag.edu/pbailey` to obtain software and notes.

You may use any books, notes, calculators, and software written in this class (by you, a classmate, or the instructor). You may not go on the internet to find software.

Prob 1	Prob 2	Prob 3	Prob 4	Prob 5	Prob 6	Prob 7	Prob 8	Total

Problem 1. Find all $x \in \mathbb{Z}_{31}$ which satisfy the given equation.

(a) $2x + 3 = 0$

(b) $x^5 - 1 = 0$

(c) $x^3 + 5x^2 - 7x + 4 = 0$

Problem 2. Let R be a finite integral domain and let $a \in R$. Define $\phi_a : R \to R$ by $\phi_a(x) = ax$.

(a) Show that the function ϕ_a is injective.

(b) Show that the function ϕ_a is surjective.

(c) Show that R is a field.

Problem 3. Let G be a group and let R be a commutative ring. Let $p \in \mathbb{Z}$ be a positive prime.

(a) Suppose that every element of g is its own inverse. Show that G is abelian.

(b) Suppose that $pa = 0$ for every $a \in R$. Show that for every $x, a \in R$ we have $(x - a)^p = x^p - a^p$.

Problem 4. Let $f \in \mathbb{Z}_7[x]$ be given by $f(x) = x^3 + 3x + 5$. Let α denote the coset represented by x in $F = \mathbb{Z}_7[x]/\langle f \rangle$. A member of F is of the form $a\alpha^2 + b\alpha + c$ for some $a, b, c \in \mathbb{Z}_5$.

(a) Show that f is irreducible.

(b) Find the inverse of α^2 in F.

Instructions for Programming Problems

Each of the four programming problems involve a block cryptosystem whose block length is 32 bits. The program `block.cpp` defines these types:

```
typedef unsigned __int8  BYT; // byte
typedef unsigned __int16 SYL; // syllable
typedef unsigned __int32 WRD; // word
typedef unsigned __int64 PHR; // phrase
typedef union
{ WRD wrd;
  SYL syl[2];
  BYT byt[4];
  BYT mat[2][2];
} BLK;
```

and contains these functions:

- `getblk`: collects four bytes from the input file into a block;
- `encblk`: encrypts the block;
- `putblk`: distributes four bytes from the block to the output file.

Your task is to produce ancillary functions, to be called by `encblk`, to implement various block cryptosystems which are modifications of ones we have studied. You will then use this program to decrypt a given file.

We describe each cryptosystem as (B, K, E), where

- B is the set of all 32-bit blocks;
- K is the key space, in each case a different subset of B;
- $E : K \to \mathrm{Sym}(B)$, where $E_k = E(k)$, so that $E_k : B \to B$ is bijective.

You are asked to decrypt the file `PROB.txc`, a ciphertext file, where `PROB` is the name of the problem. Your solutions to each programming problem should include a complete description of how you solved the problem and why it works (write on the test), and it should also include two files:

(1) The decrypted file (`PROB.txp`) (decrypted plaintext file)

(2) The software used to decrypt the file (`PROB.cpp`) (source code file)

These files should be emailed to `plbailey@saumag.edu` before the end of the examination.

Problem 5. Consider the cryptosystem (B, K, E), where

- B is viewed as the vector space $\mathbb{F}_2^{32}$
- K is $\mathbb{Z}_{32}$
- $E_k : x \mapsto x << k$, where k is the key and x is the plaintext, and $<<$ is bitwise left rotation

The file `ROTB.txc` was encrypted using the cryptosystem (B, K, E) with key 14. Decrypt.

Problem 6. Consider the cryptosystem (B, K, E), where

- B is viewed as the ring $\mathbb{Z}_{2^{32}}$
- K is B
- $E_k : x \mapsto x + k$, where k is the key and x is the plaintext

The file `SHFB.txc` was encrypted using the cryptosystem (B, K, E) with key 12345678. Decrypt.

Problem 7. Consider the cryptosystem (B, K, E), where $f \in \mathbb{F}_2[x]$ is the irreducible polynomial

$$f(x) = x^8 + x^4 + x^3 + x + 1, \text{ and}$$

- B is viewed as the ring of 2×2 matrices over $\mathbb{F}_8 = \mathbb{F}_2[x]/\langle f \rangle$ ($B_{ij} =$ `blk.mat[i][j]`)
- $K = B^*$, the set of invertible 2×2 matrices (those with nonzero determinant)
- $E_k : x \mapsto kx$, where k is the key and x is the plaintext

The file `MATB.txc` was encrypted using the cryptosystem (B, K, E) with key [GIVEN HERE]. Decrypt.

Problem 8. Consider the cryptosystem (B, K, E), where $f \in \mathbb{F}_2[x]$ is the irreducible polynomial

$$f(x) = x^{32} + x^7 + x^3 + x^2 + 1, \text{ and}$$

- B is viewed as the field of $\mathbb{F}_{2^{32}}$ realized as $\mathbb{F}_2[x]/\langle f \rangle$
- $K = B^*$, the nonzero elements of B
- $E_k : x \mapsto kx^{-1}$, where k is the key and x is the plaintext (if $x = 0$, $x \mapsto 0$)

The file `AESB.txc` was encrypted using the cryptosystem (B, K, E) with key [GIVEN HERE]. Decrypt.