Math 4613 - Cryptography - Practice Midterm
Paul L. Bailey
August 30, 2007

Part I: Mathematics

Problem 1. Complete the following definitions.

(a) Let $f : A \to B$. We say that f is *surjective* if ...

(b) Let $a, n \in \mathbb{Z}$ with $n \geq 2$. The *congruence class of a modulo n* is ...

(c) Let $(A, *)$ be a magma, and let $B, C \subset A$. Then $B * C$ means ...

(d) Let G be a finite group and let $g \in G$. The *order* of g is ...

(e) Let R be a ring and let $a \in R$. We say that a is *invertible* if ...

Problem 2. Let $a, b, c, d, n \in \mathbb{Z}$ with $n \geq 2$. Suppose $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$. Show that $ab \equiv cd \pmod{n}$.

Problem 3. Find the inverse of $\overline{123}$ in $\mathbb{Z}_{261}$.

Problem 4. Find the inverse of $A = \begin{bmatrix} \overline{5} & \overline{2} \\ \overline{11} & \overline{9} \end{bmatrix}$ in $\mathcal{M}_{2\times 2}(\mathbb{Z}_{17})$.

Problem 5. Find all $x \in \mathbb{Z}_{23}$ such that $x^2 + \overline{16}x - \overline{11} = \overline{0}$.

Problem 6. Let R be a ring and let $S, T \leq R$. Show that $S \cap T \leq R$.

Problem 7. Let G be a group and let $H, K \leq G$, with $K \leq H$. Show that

$$[G : K] = [G : H][H : K].$$

Problem 8. Let G be a group and let $H, K \leq G$. Show that

$$[G : H \cap K] = [G : H][H : H \cap K].$$

Problem 9. Let G be a group and let $H \leq G$. Suppose that $|G| = 252$ and $|H| = 21$.

(a) Show that H has an element of order 7.

(b) Show that all elements of order 7 in G are actually in H.

Problem 10. Let G be a group and let $H \leq G$. Suppose that $|G| = 285$ and $|H| = 15$.

(a) Show that H has an element of order 5.

(b) Show that all elements of order 5 in G are actually in H.

Part II: Programming

Assume that all code is preceded by the following:

```
typedef unsigned __int8     BYT;
typedef unsigned __int16    SYL;
typedef unsigned __int32    WRD;
typedef unsigned __int64    BIG;

typedef union
{ WRD wrd;
  BYT byt[4];
} BLK;

BYT rotbyt(BYT byt,int k)
{ k%=8;
  if (k<0) k+=8;
  return (byt<<k) | (byt>>(8-k)); }
```

Problem 11. Consider the cryptosystem (B, K, E) given by

- B is the set of bytes (8-bit integers);
- K is the set of bytes (8-bit integers);
- $E : K \to \mathrm{Sym}(B)$ is given by the function

```
BYT bytenc(BYT byt,WRD key)
{ BLK blk;
  blk.wrd=key;
  byt = bytrot(byt,key[0]);
  byt = byt^key[1];
  return byt; }
```

Is this balanced? closed?

Problem 12. Let B denote the set of bytes. Find the largest subset $K \subset B$ of keys on which the following functions $B \to B$ are bijective.

```
BYT ron(BYT byt,BYT key)
{ return byt + key; }

BYT bob(BYT byt,BYT key)
{ return byt * key; }

BYT ned(BYT byt,BYT key)
{ return byt / key; }

BYT tom(BYT byt,BYT key)
{ return byt & key; }

BYT sue(BYT byt,BYT key)
{ return byt | key; }

BYT tim(BYT byt,BYT key)
{ return byt ^ key; }

BYT rob(BYT byt,BYT key)
{ return byt << key; }

BYT ted(BYT byt,BYT key)
{ return bytrot(byt,key); }
```