[CSCI 55500 Cryptography] Homework 5
David Xu

1. Merkle-Hellman cryptosystem

Plaintext:

```
MiraMesa is acommunity and neighborhood in the city of San Diego, California. The city-
recognized MiraMesa Community Plan Area isroughly bounded by Interstate 15 on the east,
Interstate 805 on the west, the Los Penasquitos Canyon on the north and Marine Corps Air
Station Miramar onthe south.[2] Most of thecommunity plan area is referred to as Mira
Mesa; the community plan area also includes the neighborhoods of Sorrento Valley and
SorrentoMesa.
```

First, M and W was found by successively testing odd numbers after the initial values using the Miller-Rabin primality test with $k = 1000$. This gave $M = 203676411780221044677872131978002135 7$ and $W = 127552671440279916013021$

The Extended Euclidean Algorithm to find $W^{-1} = 71782053338341579090523712608098602 0$

This was used to calculate the items in the superincreasing knapsack:

$$a_i = W^{-1}\, b_i \bmod M$$

$$A = [57854073, 442, 885, \dots, 7583049375568, 59242573248]$$

And permutation:

$$\pi = [23, 6, 7, 36, 1, \dots, 12, 45, 27, 40, 33]$$

For each line of ciphertext y, s was determined as

$$s = W^{-1}\, y \bmod M$$

For example, the first line,

$$s = W^{-1}\, 63278191362657589762933870016882005 65 \bmod M$$
$$= 704298443550962$$

And was used to solve the superincreasing knapsack in a greedy approach to find r

$$r = 000000111110111011101110001000110000011100111 01$$

And permutated back using π to find x

$$x = 011000101110011111001100110011110011011000100 00$$

This was converted back to an integer and left padded with zeroes until the number of digits was 14

$$x = 54373856549648$$

Then each 2 characters were used in the lookup table:

$$(5,4) = M$$
$$(3,7) = i$$
$$\dots$$
$$(4,8) = s$$

Until the above plaintext was found.

[CSCI 55500 Cryptography] Homework 5
David Xu

2. Permutation Group Mapping

Plaintext:

```
In Contra, the player controls one of two armed military commandos named Bill "Mad Dog"
Rizer and Lance "Scorpion" Bean, who are sent on a mission to neutralize a terrorist group
called the Red Falcon Organization that is planning to take over the Earth. Details of the
game's setting varies between supplementary materials: the Japanese versions sets the game
in the year 2633 on the fictional "Galuga archipelago" near New Zealand,[6][7] whereas the
manual for the American NES version sets the game during the present in an unnamed South
American island. The American storyline also changes the identity of "Red Falcon" from
being the name of a terrorist organization to the name of an alien entity.[8]The main
character is equipped with a rifle with an unlimited amount of ammunition. The player can
also jump, move and fire in eight directions, as well as move or jump simultaneously while
firing. A single hit from any enemy, bullet, or other hazard will instantly kill the
player character and discard the current weapon.There are over 10 areas in the game.[6]
There are two types of stages in Contra. In addition to the standard side view stages,
Contra also features stages in which the player character is seen from behind and must
move towards the background in order to proceed. Each of these "3D maze" stages are set
inside the corridor of an enemy base in which the player must fight through the base's
defenses in order to reach the core of the base. During the 3D maze stages, the upper
screen will display a map of the base along with a time limit. Each maze stage is followed
by a "3D fixed" stage set at the core of the base, in which the player must destroy a
series of flashing sensors to expose an even larger sensor and destroy it.Contra also
features a two-player cooperative mode. Both players occupy the same screen and must
coordinate their actions. One player lagging behind can cause problems for his partner, as
the screen will not scroll onward, and a slow player can be fatal to his partner. The
European release, Gryzor, does not feature a simultaneous 2-Players mode. Instead, both
players take turns: whenever one player dies, the other gets his turn.
```

Looking at the PGM logarithmic signatures, I determined that there were 8 blocks and $r_1 = 10, r_2 = 9 \dots r_8 = 3$. This gives

$m_1 = 1$ and $p_{1j}m_1 = [0,1,2,3, \dots ,9]$, $p_{2j}m_2 = [0,10,20, \dots 80]$, $\dots$, $p_{8j}m_8 = [0,604800,1209600]$

The PGM encryption function was implemented according to the slides confirmed using the example provided for $PGM(49) = 34$. For the seed value 2000,

$$\lambda^{-1} = [0,2,6,2,0,0,0,0]$$
$$\hat{a} = [5,2,6,4,8,7,3,9,1,0]$$
$$\beta = [4,0,4,3,0,1,0,1]$$
$$PGM(2000) = k_1 = 637564$$

Then, for each 3-letter block in the ciphertext,

$$[1, L, 3] = [17,44,19] = 17 \times 95^2 + 44 \times 95 + 19 = 157624$$
$$x_i = y_i - k_i \bmod M = 157624 - 637564 = 377435$$

$$377435 = a \times 95^2 + b \times 95 + c$$
$$a = 41, b = 78, c = 0$$

Which maps to the first 3 characters [‘I’, ‘n’, ‘’].