# HW #1

Travis Collins
traviscollins@wpi.edu
ECE 578 Crytography and Data Security

September 3, 2012

## 1 Ciphertext 1

**Methodology:**
The first process was to determine what cipher was used, which was done by utilizing the attacks demonstrated in class. Starting with the easy attacks and working my way upward the attack that produced results was the Affine cipher. This was discovered by the brute force method, which is quite reasonable since there are only

$$26 * 12 = 312$$

possible permutations. This was done by loading the text into MATLAB for visual inspection and determining the values for **a** and **b**:

$$D(c) = a^{-1}(c - b)$$

**Translated:**
Alice was beginning to get very tired of sitting by her sister on the bank, and of having nothing to do: once or twice she had peeped into the book her sister was reading, but it had no pictures or conversations in it, and what is the use of a book, thought Alice without pictures or conversation?

So she was considering in her own mind (as well as she could, for the hot day made her feel very sleepy and stupid), whether the pleasure of making a daisy-chain would be worth the trouble of getting up and picking the daisies, when suddenly a White Rabbit with pink eyes ran close by her.

There was nothing so VERY remarkable in that; nor did Alice think it so VERY much out of the way to hear the Rabbit say to itself, Oh dear! Oh dear! I shall be late! (when she thought it over afterwards, it occurred to her that she ought to have wondered at this, but at the time it all seemed quite natural); but when the Rabbit actually TOOK A WATCH OUT OF ITS WAISTCOAT-POCKET, and looked at it, and then hurried on, Alice started to her feet, for it flashed across her mind that she had never before seen a rabbit with either a waistcoat-pocket, or a watch to take out of it, and

burning with curiosity, she ran across the field after it, and fortunately was just in time to see it pop down a large rabbit-hole under the hedge.

In another moment down went Alice after it, never once considering how in the world she was to get out again.

The rabbit-hole went straight on like a tunnel for some way, and then dipped suddenly down, so suddenly that Alice had not a moment to think about stopping herself before she found herself falling down a very deep well.

# 2 Ciphertext 2

**Methodology:**
I used the same process as before to determine the cipher type for the encrypted text. It reduced quickly to a Vigenere Cipher, which was quite evident by inspection of the text itself. The first step in deciphering a Vigenere Cipher is to determine the keyword length. This was done by finding the longest repeated words in the text, determining their distance apart, and finally taking the "GCD" of that distance. The keyword then was determined to be 5. The next step was to determine the shift distances or the keyword itself. This was done by assume original words for encrypted text, measuring the distance of the ciphered text letter to the plaintext letter for repeated or assumed repeated words. These shifts were determined to be:

$$7, 16, 9, 2, 11$$

or the keyword "krypt".

**Translated:**
Down, down, down. Would the fall NEVER come to an end! I wonder how many miles Ive fallen by this time? she said aloud. I must be getting somewhere near the centre of the earth. Let me see: that would be four thousand miles down, I think– (for, you see, Alice had learnt several things of this sort in her lessons in the schoolroom, and though this was not a VERY good opportunity for showing off her knowledge, as there was no one to listen to her, still it was good practice to say it over) –yes, thats about the right distance–but then I wonder what Latitude or Longitude Ive got to? (Alice had no idea what Latitude was, or Longitude either, but thought they were nice grand words to say.)

Presently she began again. I wonder if I shall fall right THROUGH the earth! How funny itll seem to come out among the people that walk with their heads downward! The Antipathies, I think– (she was rather glad there WAS no one listening, this time, as it didnt sound at all the right word) –but I shall have to ask them what the name of the country is, you know. Please, Maam, is this New Zealand or Australia? (and she tried to curtsey as she spoke–fancy CURTSEYING as youre falling through the air! Do you think you could manage it?) And what an ignorant little girl shell think me for asking! No, itll never do to ask: perhaps I shall see it written up somewhere.

Down, down, down. There was nothing else to do, so Alice soon began talking again. Dinahll miss me very much to-night, I should think! (Dinah was the cat.) I hope theyll remember her saucer of milk at tea-time. Dinah my dear! I wish you were down here with me! There are no mice in the air, Im afraid, but you might catch a bat, and thats very like a mouse, you know. But do cats eat bats, I wonder? And here Alice began to get rather sleepy, and went on saying to herself, in a dreamy sort of way, Do cats eat bats? Do cats eat bats? and sometimes, Do bats eat cats? for, you see, as she couldnt answer either question, it didnt much matter which way she put it. She felt that she was dozing off, and had just begun to dream that she was walking hand in hand with Dinah, and saying to her very earnestly, Now, Dinah, tell me the truth: did you ever eat a bat? when suddenly, thump! thump! down she came upon a heap of sticks and dry leaves, and the fall was over.

Alice was not a bit hurt, and she jumped up on to her feet in a moment: she looked up, but it was all dark overhead; before her was another long passage, and the White Rabbit was still in sight, hurrying down it. There was not a moment to be lost: away went Alice like the wind, and was just in time to hear it say, as it turned a corner, Oh my ears and whiskers, how late its getting! She was close behind it when she turned the corner, but the Rabbit was no longer to be seen: she found herself in a long, low hall, which was lit up by a row of lamps hanging from the roof.

# 3 Matlab Code

### Affine Decoder

```
1 %affine decoder
2 %fid=fopen('R:\git¬1\ECE578\hw1.txt');
```

```
fid=fopen('¬/Git/ECE578/hw1.txt');
txt=fread(fid);
%remove beginning txt
txt=txt(298:1968);

%F=a*m+b
%FOUND: a=7,b=13
%a=1:2:15;

txt_saved=txt;
for a=1:2:26
for b=0:25
    txt=txt_saved;
    for i=1:length(txt)
        if (txt(i)≥65 && txt(i)≤65+25)
            %remove bias
            temp=txt(i);
            temp=temp-65;
            [¬,a_i,¬]=gcd(a,26);
            a_i=mod(a_i,26);
            temp=mod(round(a_i*(temp-b)),26);
            txt(i)=round(temp)+65;
        elseif(txt(i)≥97 && txt(i)≤97+25)
            %remove bias
            temp=txt(i);
            temp=temp-97;
            [¬,a_i,¬]=gcd(a,26);
            a_i=mod(a_i,26);
            temp=mod(round(a_i*(temp-b)),26);
            txt(i)=round(temp)+97;
        end
    end
    %Look at sample output
    %char(txt(1:30))'
    %b
    %a
    %pause
end
end

%break
%converted txt
for a=7
for b=13
    txt=txt_saved;
```

```
48      for i=1:length(txt)
49          if (txt(i)≥65 && txt(i)≤65+25)
50              %remove bias
51              temp=txt(i);
52              temp=temp-65;
53              [¬,a_i,¬]=gcd(a,26);
54              a_i=mod(a_i,26);
55              temp=mod(round(a_i*(temp-b)),26);
56              txt(i)=round(temp)+65;
57          elseif(txt(i)≥97 && txt(i)≤97+25)
58              %remove bias
59              temp=txt(i);
60              temp=temp-97;
61              [¬,a_i,¬]=gcd(a,26);
62              a_i=mod(a_i,26);
63              temp=mod(round(a_i*(temp-b)),26);
64              txt(i)=round(temp)+97;
65          end
66      end
67
68  end
69  end
70
71  txt_file=char(txt);
72  %save to file
73  fid2 = fopen('¬/Git/ECE578/hw1_p1.txt','w');
74  fprintf(fid2,txt_file);
```

### Vigenere Decoder

```
1   %letter shifter
2   fid=fopen('¬/Git/ECE578/hw1.txt');
3   txt=fread(fid);
4   %remove beginning txt
5   txt=txt(1989:end);
6
7
8
9   shifts=[7 16 9 2 11];
10  txt(1)=mod((txt(1)-65)+shifts(2),26)+65;
11  txt(2)=mod((txt(2)-97)+shifts(3),26)+97;
12  txt(3)=mod((txt(3)-97)+shifts(4),26)+97;
13  txt(4)=mod((txt(4)-97)+shifts(5),26)+97;
```

```
14
15 j=1;
16 shift=0;
17 for i=1:length(txt)
18
19     if (txt(i)≥65 && txt(i)≤65+25)||(txt(i)≥97 && ...
           txt(i)≤97+25)
20         shift=shift+1;
21     end
22     if shift≥5
23     if (txt(i)≥65 && txt(i)≤65+25)
24             %remove bias
25             temp=txt(i);
26             temp=temp-65;
27             temp=mod(temp+shifts(j),26);
28             txt(i)=round(temp)+65;
29             shift=0;
30         elseif(txt(i)≥97 && txt(i)≤97+25)
31             %remove bias
32             temp=txt(i);
33             temp=temp-97;
34             temp=mod(temp+shifts(j),26);
35             txt(i)=round(temp)+97;
36             shift=0;
37         end
38     end
39
40
41 end
42 j=2;
43 %char(txt(1:30))'
44 shift=-1;
45 for i=1:length(txt)
46
47     if (txt(i)≥65 && txt(i)≤65+25)||(txt(i)≥97 && ...
           txt(i)≤97+25)
48         shift=shift+1;
49     end
50     if shift≥5
51     if (txt(i)≥65 && txt(i)≤65+25)
52             %remove bias
53             temp=txt(i);
54             temp=temp-65;
55             temp=mod(temp+shifts(j),26);
56             txt(i)=round(temp)+65;
```

```
            shift=0;
        elseif(txt(i)≥97 && txt(i)≤97+25)
            %remove bias
            temp=txt(i);
            temp=temp-97;
            temp=mod(temp+shifts(j),26);
            txt(i)=round(temp)+97;
            shift=0;
        end
    end


end
j=3;
%char(txt(1:30))'
shift=-2;
for i=1:length(txt)

    if (txt(i)≥65 && txt(i)≤65+25)||(txt(i)≥97 && ...
       txt(i)≤97+25)
        shift=shift+1;
    end
    if shift≥5
    if (txt(i)≥65 && txt(i)≤65+25)
            %remove bias
            temp=txt(i);
            temp=temp-65;
            temp=mod(temp+shifts(j),26);
            txt(i)=round(temp)+65;
            shift=0;
        elseif(txt(i)≥97 && txt(i)≤97+25)
            %remove bias
            temp=txt(i);
            temp=temp-97;
            temp=mod(temp+shifts(j),26);
            txt(i)=round(temp)+97;
            shift=0;
        end
    end


end
j=4;
%char(txt(1:30))'
shift=-3;
```

```
101
102 for i=1:length(txt)
103
104     if (txt(i)≥65 && txt(i)≤65+25)||(txt(i)≥97 && ...
        txt(i)≤97+25)
105         shift=shift+1;
106     end
107     if shift≥5
108     if (txt(i)≥65 && txt(i)≤65+25)
109             %remove bias
110             temp=txt(i);
111             temp=temp-65;
112             temp=mod(temp+shifts(j),26);
113             txt(i)=round(temp)+65;
114             shift=0;
115         elseif(txt(i)≥97 && txt(i)≤97+25)
116             %remove bias
117             temp=txt(i);
118             temp=temp-97;
119             temp=mod(temp+shifts(j),26);
120             txt(i)=round(temp)+97;
121             shift=0;
122         end
123     end
124
125
126 end
127 j=5;
128 %char(txt(1:30))'
129 shift=-4;
130
131 for i=1:length(txt)
132
133     if (txt(i)≥65 && txt(i)≤65+25)||(txt(i)≥97 && ...
        txt(i)≤97+25)
134         shift=shift+1;
135     end
136     if shift≥5
137     if (txt(i)≥65 && txt(i)≤65+25)
138             %remove bias
139             temp=txt(i);
140             temp=temp-65;
141             temp=mod(temp+shifts(j),26);
142             txt(i)=round(temp)+65;
143             shift=0;
```

```
144         elseif(txt(i)≥97 && txt(i)≤97+25)
145             %remove bias
146             temp=txt(i);
147             temp=temp-97;
148             temp=mod(temp+shifts(j),26);
149             txt(i)=round(temp)+97;
150             shift=0;
151         end
152     end
153
154
155 end
156
157 txt_file=char(txt);
158 %save to file
159 fid2 = fopen('¬/Git/ECE578/hw1_p2.txt','w');
160 fprintf(fid2,txt_file);
```