MATH220

Discrete Mathematics and Cryptography

Tutorial 1 **Week starting 24 February 2020**

---

1. You intercept the ciphertext `KRON`, which was encrypted using an affine function. You know that `do` is the first two letters of the plaintext. Find the encryption function and the plaintext. (Use the numeric values $a \to 00, b \to 01, \ldots, z \to 25$.)

2. Suppose you try to use the affine function $2x + 1$ to encrypt. Find two letters that encrypt to the same ciphertext letter.

3. Alice and Bob have each generated their own one-time pad keys, k_A and k_B. Alice encrypts an ASCII message m with her key and sends it to Bob. I.e. $c_1 = m + k_A \mod 2$ bitwise. You intercept

$$c_1 = 11101011\ \ 10001010\ \ 11110010\ \ 01111101\ \ 11000110.$$

Bob then further encrypts c_1 with his key and send it back to Alice. You intercept

$$c_2 = 10110100\ \ 11011011\ \ 01000001\ \ 10101011\ \ 10001100.$$

Finally Alice removes her encryption from c_2 by setting $c_3 = c_2 + k_A \mod 2$ bitwise. She sends this to Bob. You intercept

$$c_3 = 00010111\ \ 00111000\ \ 10010011\ \ 10000011\ \ 00001001.$$

Since c_3 is now only encrypted with Bob's key, Bob can now decrypt to obtain the original message. Can you also recover the message, and if so what is it?

4. Let $a, b, c \in \mathbb{Z}$. Use the definition of divisibility to obtain the following results.

(a) If $a \mid b$ and $b \mid c$, then $a \mid c$.

(b) If $a \mid b$, then $ac \mid bc$ for all c.

(c) If $a \mid b$ and $a \mid c$, then $a \mid (mb + nc)$ for all integers m and n.

(d) If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.

(e) If $a \mid b$ and $b \mid a$, then $a = \pm b$.

5. Find all integers n (positive or negative) such that $n^2 - n$ is prime.

6. (a) Write each of 168 and 192 as a product of primes.

(b) Using the prime factorisations in (a), determine the number of distinct positive divisors of 168 and 192, and $\gcd(168, 192)$.

7. (a) Show that if $n \geq 2$ and n is non-prime, then there is a prime p such that $p \mid n$ and $p^2 \leq n$.

(b) Using (a), show that if 467 is not a prime, then it has a prime divisor $p \leq 19$.

(c) Deduce that 467 is a prime.

8. If $n > 1$, show that the n consecutive integers

$$(n+1)! + 2, (n+1)! + 3, \ldots, (n+1)! + (n+1)$$

are all composite. (This shows that there are arbitrarily large gaps between primes.)

9. Playfair Cipher. In 1854, Sir Charles Wheatstone invented the cipher which later became known as "Playfair" after his friend Baron Playfair of St. Andrews, who popularised and promoted the cipher. Its simplicity and its cryptographic strength compared to simple substitution ciphers made it an immediate success as a field cipher. It was used by the British in the Boer War and the First World War, and by several armed forces as an emergency back-up cipher in the Second World War. (When Lt. John F. Kennedy's PT-109 was sunk by a Japanese cruiser in the Solomon Islands, he made it ashore on Japanese-controlled Plum Pudding Island and was able to send an emergency message in Playfair from an Allied coast-watcher's hut to arrange the rescue of the survivors from his crew.)

Preparing the Playfair square

To use the Playfair cipher, you first choose a *keyword or phrase*. Any repeated letters are deleted. So, if your key is "manchester", it will become "manchestr". You then write it, left to right, in a five-by-five square, which combines `i` and `j` in one cell. Once you've done this, you then fill in the rest of the square with the rest of the letters in alphabetical order. This gives you the Playfair square

```
m  a  n  c  h
e  s  t  r  b
d  f  g i/j k
l  o  p  q  u
v  w  x  y  z
```

Enciphering

Next we need to prepare the plaintext message for encryption. To encrypt "this secret message is encrypted", break it up into two-letter groups (ignore blanks). If both letters in a pair are the same, insert an `x` between them. If there is only one letter in the last group, add an `x` to it.

We then have

```
th is se cr et me sx sa ge is en cr yp te dx
```

We now use the Playfair square to encrypt *each two-letter group*. Find the `t` and `h` in the square and locate the letters at opposite corners of the rectangle they form

```
.  .  n  .  h
.  .  t  .  b
.  .  .  .  .
.  .  .  .  .
.  .  .  .  .
```

Replace `th` with those letters, *starting with the letter on the same row as the first letter of the pair*. `th` becomes `BN`. Continue this process with each pair of letters.

```
th is se cr et me sx sa ge is en cr yp te dx
BN FR
```

Now we notice that `s` and `e` are in the same row. In this case, we take the letter immediately to the right of each letter of the pair, so that `se` becomes `ts`.

```
.  .  .  .  .
e  s  t  .  .
.  .  .  .  .
.  .  .  .  .
.  .  .  .  .
```

```
th is se cr et me sx sa ge is en cr yp te dx
BN FR TS
```

(If one letter occurs at the end of a row, treat the row *cyclically* so that the next letter along is at the start of the row. Similarly for columns as described below.)

Next we see that `c` and `r` are in the same column. Use the letter

```
.  .  .  c  .
.  .  .  r  .
.  .  . i/j .
.  .  .  .  .
.  .  .  .  .
```

immediately below each of these letters, so that `cr` becomes `ri`. This is the last special case, and the encryption proceeds without further incident.

```
th is se cr et me sx sa ge is en cr yp te dx
BN FR TS RI SR ED TW FS DT FR TM RI XQ RS GV
```

Deciphering

To decrypt the message, simply reverse the process. If the two letters are in different rows and columns, take the letters in the opposite corners of their rectangle. If they are in the same row, take the letters to the left. If they are in the same column, take the letters above each of them.

Problem[1]

You are a well-known cryptanalyst and you have just received the following memo.

Memo:

To: Hut 6d, Bletchley Park

From: Col. W. T. Tutte, Military Attache, Cafe 101, MSCS[2]

This message was received by an intercept station in Scotland. The frequency and format indicate that it is a most urgent message from one of our agents who landed a week ago in Norway. His controllers have been unable to read it. Although it clearly uses his backup cipher, the Playfair, the keys assigned to him do not work. We cannot reach him before his normal scheduled transmission in three weeks, so we urgently request that you attempt to decrypt this and let us know the contents. In case it helps, he is carrying materials to assist a previously dropped team in their work regarding the Norsk Hydro facility at Rjukan. His recognition code might appear in the message: It is "beware ice weasels". If he is operating under duress, he will not use it and instead will include the phrase "red penguin frenzy". He will use "stop" between sentences and "end" at the end.

Received message:

```
FVLYP IPGLU LYPQH FFSDE MDHEV OKNCB GEPSM FNCKY
GSSBU PURKI UFOHH QZRYS FUHEL CXSAP BUOVA EIFYL
UPWED SWGFK ZBFGE GUIHL UPQEU FPUBD KBOVK YFTZP
QUMRB OLUHN NHNRW MAQPA BCFIP SMHKB UHEDO VHEMO
SGIFB CFKVU GBBGK CXXXX
```

It is vital that this message be broken as soon as possible.

[1]This cipher is an amalgam of several real incidents during the second world war. For more background, including the fate of the expedition, see *Between Silk and Cyanide: A Codemaker's War 1941-1945* by Leo Marks (Free Press, 1999).

[2]Most Secret Cipher School

Hints

The Playfair cipher has two characteristic properties which are of great use in deciphering.

(I) No letter can be enciphered to itself.

(II) If `ab` is enciphered to `XY`, then `ba` is enciphered to `YX`.

Look first at "beware ice weasels". It may be segmented as

```
-b ew ar ei ce we as el s-
```

or as

```
be wa re ic ew ea se ls
```

In the second case, it might appear either

(i) at the beginning of the message or

(ii) at the end, in which case it will appear as

```
st op be wa re ic ew ea se ls en dx
```

or

(iii) inside the message, in which case it must be in the form

```
st op be wa re ic ew ea se ls st op
```

(a) Check which (if any) of these four possibilities can occur.

(b) Consider the possible segmentations of the phrase "red penguin frenzy" and, as before, find any allowable ones. Use the information you now have, to construct as much of the Playfair square as you can.

(c) Find the original key phrase and decipher the whole message.