MATH 4161 Mathematics of Cryptography **Lecture 2**
LECTURE JOE TRAN

1. Test Dates

- Test 1: Thursday, February 1 (Probability Theory and Cryptosystems)
- Test 2: Tuesday March 5 (Information Theory)
- Test 3: Thursday, March 21 (Number Theory and Modern Cryptography)

2. Caesar and Vigenere Transformations

Example 1. Given the plaintext ATTACK encrypt it with the Caesar key G.

Since our key is G, then the Caesar shift with key G is as follows:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F

Therefore, our encrypted text is GZZGIQ.

Example 2. Given the plaintext ATTACK, encrypt it with the keyword GEM.

Since our keyword is GEM, then we have the following shifts performing as follows:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L

So from the above table, we have the encrypted text given by GXFGGW.

There would be a shorter way to go around this, if we are familiar with modular arithmetic. That is, recall that a **mod** n is the remainder when a is divided by n. In this case, since we have 26 characters in our alphabet system, then $n = 26$. Thus, in this case,

$$a \textbf{ mod } 26 = r$$

where $a = 26q + r$, and $0 \leq r < 26$.

Example 3. Suppose T is Caesar shifted by G. Note that the position of each alphabet is given as follows

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

So T is in the 19th position, while G is in the 6th position, and so

$$19 +_{26} 6 = 19 + 6 \textbf{ mod } 26 = 25$$

Here, recall the operation $+_n$ means the addition modulo n, i.e. for $a, b \in \mathbb{Z}_n$,

$$a +_n b = a + b \textbf{ mod } n$$

Example 4. Following from Example 3, suppose now we want to encrypt ATTACK with keyword GEM. Since

$$\begin{array}{cccccc} \text{A} & \text{T} & \text{T} & \text{A} & \text{C} & \text{K} \\ \Downarrow & \Downarrow & \Downarrow & \Downarrow & \Downarrow & \Downarrow \\ 0 & 19 & 19 & 0 & 2 & 10 \end{array}$$

and since

$$\begin{array}{ccc} \text{G} & \text{E} & \text{M} \\ \Downarrow & \Downarrow & \Downarrow \\ 6 & 4 & 12 \end{array}$$

Then

$$\begin{aligned} A &: 0 +_{26} 6 = 6 \\ T &: 19 +_{26} 4 = 23 \\ T &: 19 +_{26} 12 = 5 \\ A &: 0 +_{26} 6 = 6 \\ C &: 2 +_{26} 4 = 6 \\ K &: 10 +_{26} 12 = 22 \end{aligned}$$

So since

$$\begin{array}{cccccc} \text{A} & \text{T} & \text{T} & \text{A} & \text{C} & \text{K} \\ \text{G} & \text{E} & \text{M} & \text{G} & \text{E} & \text{M} \\ \hline 6 & 23 & 5 & 6 & 6 & 22 \\ \hline \text{G} & \text{X} & \text{F} & \text{G} & \text{G} & \text{W} \end{array}$$

which is the same as in Example 2.

Sample Code 1. The following is an example of how to encrypt a string of letters into ciphertext.

```
def encrypt(plaintext, shift):
ans = ""
for i in range(len(plaintext)):
    ch = plaintext[i]
    if ch == " ":
        ans += " "
    elif (ch.isupper()):
        ans += chr((ord(ch) + shift - 65) % 26 + 65)
    else:
        ans += chr((ord(ch) + shift - 97) % 26 + 97)
return ans

def main():
    plaintext = input("Enter String: ")
    shift = int(input("Enter Shift: "))
    encrypt(plaintext, shift)

    print(plaintext, shift, encrypt(plaintext, shift))

main()
```

3. Rectangular Transformations

Note that a key in this case, is called a *permutation*.

Example 5. Consider the string given by “Why did you bring that book I did not want to be read to out of from up for?”, and so consider

3	1	4	2	7	5	6
W	H	Y	D	I	D	Y
O	U	B	R	I	N	G
T	H	A	T	B	O	O
K	T	H	A	T	I	D
I	D	N	T	W	A	N
T	T	O	B	E	R	E
A	D	T	O	O	U	T
O	F	F	R	O	M	U
P	F	O	R	W	A	Y

The numbers on the top row represent the position of each column. So, now: HUHTD TDFFD RTATB ORRWO TKITA OP ... TWEOOW.

Example 6. The following message was encrypted with rectangular transposition. Decrypt it given that the letters X and P are adjacent in the plaintext.

OTIEN RETXM LRRWN RTRCC HPEER IEIAO

So we first put the 5-grams into columns.

O	R	L	R	H	I
T	E	R	T	P	E
I	T	R	R	E	I
E	X	W	C	E	A
N	M	N	C	R	O

But here, the X and P are not next to each other, so this rectangle would be considered invalid. Notice that the rectangular table is 5 × 6, but are there other possibilities? What if we consider 6 × 5? Then

O	E	R	C	R
T	T	W	C	I
I	X	N	H	E
E	M	R	P	I
N	L	T	E	A
R	R	R	E	O

Now we see that the column with the X and the column with the P are not so that the X and P are not next to each other. But, if we apply some transpositions, moving the second column to the last column, and the fourth column to the first column, and applying other transformations

C	O	R	R	E
C	T	W	I	T
H	I	N	E	X
P	E	R	I	M
E	N	T	A	L
E	R	R	O	R