MATH 4161 Mathematics of Cryptography **Lecture 3**
LECTURE JOE TRAN

Contents

1 Rectangular Transposition Keys

A rectangular transposition key is the number of columns. For example, 4132576 is a permutation. Alternatively, use a key word BATHROOM, in which case,

B	A	T	H	R	O	O	M
2	1	8	3	7	5	6	4

2 Playfair

Key:

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

Plaintext:

382 Robertson Dr, West Hollywood

Whenever we see numbers in the plaintext, we convert them into their word, i.e. 3 = three. Some rules:

1. Stick with A-Z
2. Replace J with I
3. Convert any numbers to text
4. Break into 2-grams and no adjacent letters equal. Insert a Q to make sure that no 2-gram has equal letters.

From the above,

TH RE EQ EI GH TQ TW OR OB ER TS ON DR WE ST HO LQ LY WO OD

Then we obtain, in order,

qo wb dr na lp ur ry kt kf bw ut mi eq eb tu kp hv fv yk hi

Some other rules to keep in mind:

1. If two letters in the key are in the same row, then move to the right for the encrypted 2-gram. For example, take B and F. Because they are in the same row, then move to the right to obtain the encrypted 2-gram cg.

2. If two letters in the key are in the same column, then move down for the encrypted 2-gram. For example, take B and R. Because they are in the same row, then move down to obtain the encrypted 2-gram kw.

3. If two letters are in opposite corners,

   (a) Ex. Considering RF in the 2-gram. Move the R to the T and move the F to the B to obtain the encrypted 2-gram TB.

   (b) Ex. Considering BT in the 2-gram. Move the B to the F and move the T to the R to obtain the encrypted 2-gram FR.

4. If two letters are in the same row, but a letter goes outside the box, then wrap it around. For example, consider RN in the 2-gram. Then shifting to the right gives PL because the N moves outside the box, so we wrap it back to the first letter of the row, which is L.

5. If two letters are in the same column, but a letter goes outside the box, then wrap it around. For example, consider BW in the 2-gram. Then moving down gives KE because W moves outside the box, so we wrap it back to the first letter of the column, which is E.

Example 1. Given the phrase: Office floor plans and given the plaintext Massive heart attack, then our key is

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

Then splitting the plaintext into two grams:

M	A	S	Q	S	I	V	E	H	E	A	R	T	A	T	Q	T	A	C	K
T	R	D	K	D	O	Z	O	V	N	N	P	Y	G	U	T	Y	G	O	T

So the ciphertext is tr dk do zo vn np yg ut yg ot.

For playfair, the key must be a 5 × 5 box.

3 Homophonic Substitution

This one is called the homophonic substitution, which is similar to the Caesar substitution.

	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
S	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	1	2	3	4	5	6	7	8
T	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	1	2	3	4	5	6	7
A	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
N	14	15	16	17	18	19	20	21	22	23	24	25	1	2	3	4	5	6	7	8	9	10	11	12	13

This one is called a polyalphabet substitution.

	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
S	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	1	2	3	4	5	6	7	8
T	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	26	27	28	29	30	31	32
A	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
N	89	90	91	92	93	94	95	96	97	98	99	100	76	77	78	79	80	81	82	83	84	85	86	87	88

Here, our key is STAN. Given the plaintext Then why did you turn some of us inside out?, we can convert this using the table above.

```
T H E N  W HYD IDYO UTUR NSOM EOFU SINS IDEO UT?
82 16 55 45  85 16 ...
```

Or, given the ciphertext 69-16-9-2-85-33-81-35-51-25-61-40-13-1-45-93-85-20-64-77 reads that was carlhesnewmoo (??)