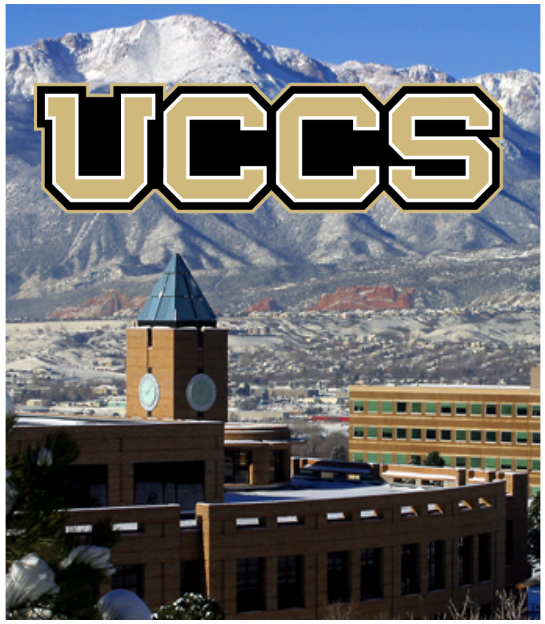


Symmetric Cryptography

Classical Cipher: Transposition

Sang-Yoon Chang, Ph.D.

Module Objectives:
Classical Cipher: Transposition

Transposition Cipher, e.g.,
Rail-Fence and Transposition

Transposition Cipher Security

Product Cipher

Transposition Cipher

Re-arrange the order/positions of the alphabets without altering their values

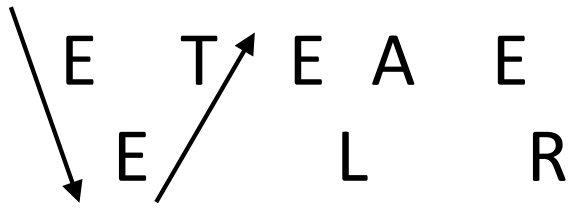
Rail Fence Cipher

List the plaintext alphabets diagonally over a number of rows, and then retrieve alphabets row by row

Rail Fence Cipher (3 Rows)

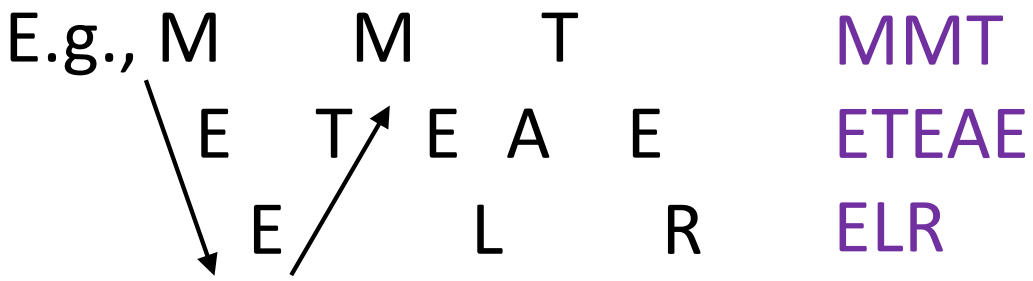
List the plaintext alphabets diagonally over a number of rows, and then retrieve alphabets row by row

E.g., M M T



Rail Fence Cipher (3 Rows)

List the plaintext alphabets diagonally over a number of rows, and then retrieve alphabets row by row



Rail Fence Cipher (3 Rows)

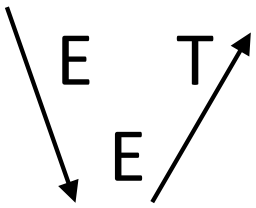
List the plaintext alphabets diagonally over a number of rows, and then retrieve alphabets row by row

Ciphertext: MMTETEAEELR

E.g., M M T MMT

E T E A E ETEAE

E L R ELR



Permutation Cipher

List the plaintext alphabets row by row and retrieve the ciphertext alphabets column by column

Key determines the column order and is a permutation of a set of size *n*

Key length (*n*) corresponds to *n* columns

Permutation Cipher Example

Key = [4 3 1 2] // Key length specifies
the number of columns

M	E	E	T
M	E	L	A
T	E	R	

Permutation Cipher Example

Key = [4 3 1 2] // Key length specifies the number of columns

M	E	E	T
M	E	L	A
T	E	R	x // Can also fill with arbitrary alphabets

Permutation Cipher Example

Key = [4 3 1 2] // Key length specifies the number of columns

n=4

M	E	E	T
M	E	L	A
T	E	R	

Permutation Cipher Example

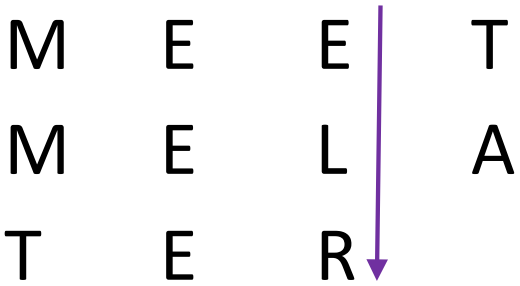
Key = [4 3 1 2] // Key length specifies *n*=4 the number of columns

M	E	E	T
M	E		
T	E		

If Key is *n* alphabets long, there are *n*! possible keys where $n! = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 1$

Permutation Cipher Example

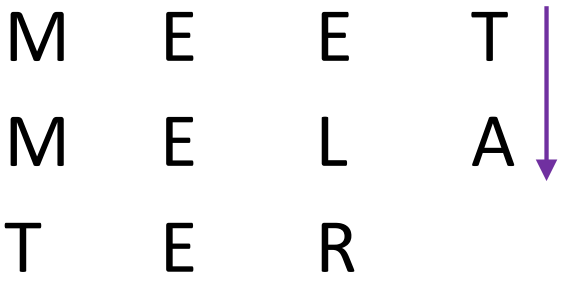
Key = [4 3 1 2]



Ciphertext: ELR

Permutation Cipher Example

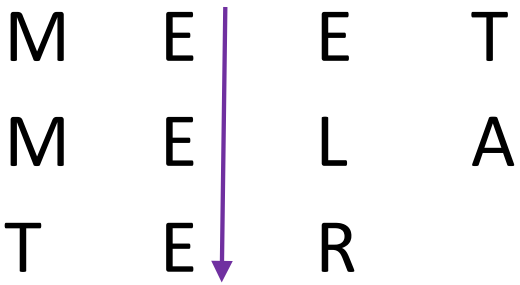
Key = [4 3 1 2]



Ciphertext: ELRTA

Permutation Cipher Example

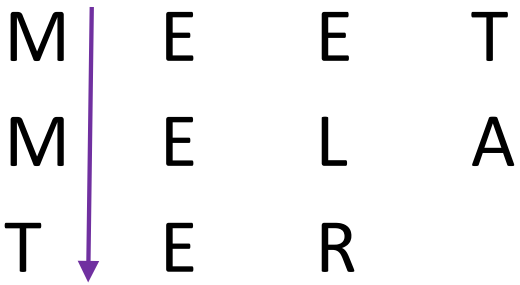
Key = [4 3 1 2]



Ciphertext: ELRTAEEE

Permutation Cipher Example

Key = [4 3 1 2]



Ciphertext: ELRTAEEEMMT

Permutation Cipher and Transposition Cipher

Any transposition cipher can be generalized by a permutation cipher with a key of length equal to the plaintext

One row in the matrix in this case

Transposition Cipher Security

The alphabet values do not change

=> The frequency distribution is the same

Transposition Cipher Security

The alphabet values do not change

=> The frequency distribution is the same

Vulnerable to cryptanalysis,

e.g., known/chosen plaintext attack

Permutation Cipher Example

Key = [4 3 1 2]

M	E	E	T
M	E	L	A
T	E	R	

Ciphertext: ELRTAEEEMMT

Known Plaintext Attack

Key = [? ? ? ?]

M E L T

M E L A

T E R

"Where does MMT occur?"

Ciphertext: ELRTAEEEMMT

Known Plaintext Attack

Key = [4 ? ? ?]

M E

M E

T E R

"Where does MMT occur?"

Ciphertext: ELRTAEEEMMT

Known Plaintext Attack

Key = [4 3 ? ?]

M	E	E	T
M	E	L	A
T	E	R	

Ciphertext: ELRTAEEEMMT

Known Plaintext Attack

Key = [4 3 1 2]

M	E	E	T
M	E	L	A
T	E	R	

Ciphertext: ELRTAEEEMMT

Known Plaintext Attack

Key = [4 3 1 2]

M	E	E	T
M	E	L	A
T	E	R	?
…	…		

ELR…TA?…EEE…MMT…

Chosen Plaintext Attack

Key = [? ? ? ?]

X	Y	Z	A
B	C	D	E
F	G	H	I

Try chosen plaintext
XYZABCDEFGHI

Ciphertext: ZDHAEIYCGXBF

Chosen Plaintext Attack

Key = [4 3 1 2]

X	Y	Z	A
B	C	D	E
F	G	H	I

Try chosen plaintext

XYZABCDEFGHI

Ciphertext: **Z**DH**A**EI**Y**CG**X**BF

Product Cipher

Combinations of substitution ciphers
and transposition ciphers in succession

Improve security

Modern ciphers use product ciphers