A History of Cryptography and Cryptanalysis

Christopher Colahan
Simpson College

Transposition Ciphers

- Rearrange text
- Common example Columnar Cipher

[6, pg. 12]

Columnar Transposition Cipher

Plaintext: THIS IS A SECRET MESSAGE

T	H	I	S	I
S	A	S	E	C
R	E	T	M	E
S	S	A	G	E

Ciphertext: TSRS HAES ISTA SEMG ICEE

Monoalphabetic Substitution Ciphers

Monoalphabetic substitution ciphers replace each character in the plaintext with another character

- Shift Cipher

$$E(p_i, k) = p_i + k \pmod{n}$$

$$D(c_i, k) = c_i - k \pmod{n}$$

- Substitution Cipher
  - Each character from the plaintext is mapped to a character from a table to obtain the plaintext

Polyalphabetic Substitution Ciphers

- Vigenère Cipher
  - 26 alphabets
  - encrypt plaintext character p and key character k by finding character in p column and k row

$$E(p_i, k_j) = p_i + k_j \pmod{26} = c_i$$

$$D(c_i, k_j) = c_i - k_j \pmod{26} = p_i$$

Vigenère Square

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

Vigenère Cipher Example

Plaintext: SEND SUPPLIES AT ONCE
Key: CODE

S	E	N	D	S	U	P	P	L	I	E	S	A	T	O	N	C	E
C	O	D	E	C	O	D	E	C	O	D	E	C	O	D	E	C	O
U	S	Q	H	U	I	S	T	N	W	H	W	C	H	R	R	E	S

Ciphertext: USQHUISTNWHWCHRRES

Frequency Analysis

Substitution ciphers can be broken by using a a statistical technique called frequency analysis

- Shift cipher
  - Compare character frequency chart or graph to sample of english
- Vigenère cipher
  - Fist find length of key using frequency analysis
  - find each character in key using frequency analysis

Character Frequency Chart for English

Letter	Percentage	Letter	Percentage	Letter	Percentage
a	8.2	j	0.2	s	6.3
b	1.5	k	0.8	t	9.1
c	2.8	l	4.0	u	2.8
d	4.3	m	2.4	v	1.0
e	12.7	n	6.7	w	2.4
f	2.2	o	7.5	x	0.2
g	2.0	p	1.9	y	2.0
h	6.1	q	0.1	z	0.1
i	7.0	r	6.0		

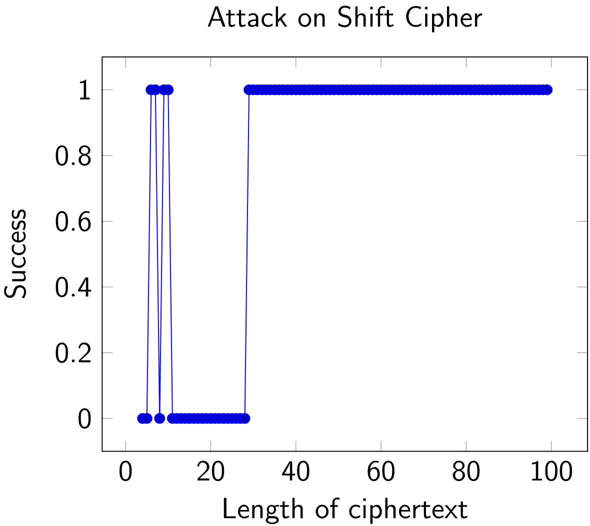
[7, pg. 19]

Character Frequency Chart for Ciphertext

The sample text was encoded using a shift cipher

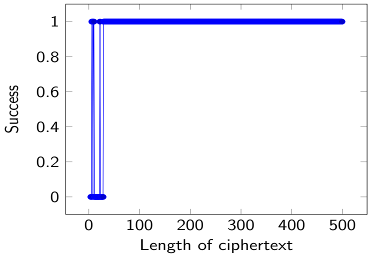
Letter	Percentage	Letter	Percentage	Letter	Percentage
a	8.4	j	0.1	s	2.5
b	1.4	k	2.3	t	6.0
c	0.0	l	0.0	u	6.5
d	4.6	m	8.3	v	0.3
e	5.8	n	1.7	w	1.3
f	9.7	o	1.9	x	4.0
g	3.2	p	5.4	y	2.4
h	0.7	q	11.2	z	7.5
i	3.0	r	1.8		

Attack on Shift Cipher

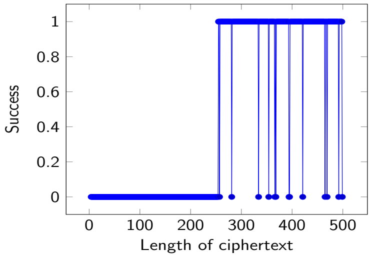


Attack on Vigenère Cipher

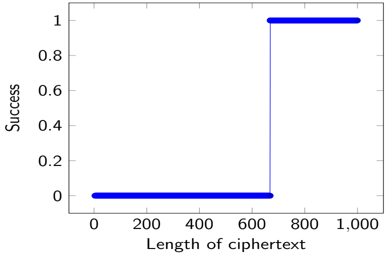
Attack on Vigenère Cipher With Key Length 1



Attack on Vigenère Cipher With Key Length 2



Attack on Vigenère Cipher With Key Length 5



One Time Pad

The one time pad cipher is a version of the Vigenère cipher where

- The key is the same length as the plaintext
- The key is random, and
- The key is not reused for multiple encryptions

There is no statistical analysis that can be applied to the ciphertext to break the one time pad [4, pg. 393]

One Way Hashes

A one way hash is an algorithm or function H that takes a plaintext p and converts it to ciphertext c, where computing $H^{-1}(c) = p$ is much more computationally difficult than computing $H(p) = c$

Attacks

- Brute Force
- Birthday
- Statistical
- Man in the Middle
- Side-Channel

Brute Force Attack

- Try every possible key
- Not efficient or practical against most ciphers

A brute force attack tries every possible key

Birthday Attack

Given a ciphertext c where $H(p) = c$, a birthday attack on a one way hash is to find p' where $H(p) = H(p')$ [6]

Man in the Middle Attack

Attack on public key cryptography. An attacker can control all communications if there is no authentication.

Side-Channel Attack

Using information available from other sources than the ciphertext and plaintext, an attacker could determine information about the key to a cipher

- Timing
- Power consumption
- Fault

Future Research

- Differential cryptanalysis
- Attacks on recently broken ciphers and hashing algorithms
- Man in the middle and side-channel attacks

References I

Hagai Bar-El.
Introduction to Side Channel Attacks.
Discretix Technologies Ltd.

Whitfield Diffie and Matrin E. Hellman.
New Directions in Cryptography.
IEEE Transactions on Information Theory, November 1976.

Katrina Falkne and Yuval Yarom.
Flush+Reload: A High Resolution, Low Noise, L3 Chache Side-Channel Attack.
In *Proceedings of the 23rd USENIX Security Symposium*, pages 719–732, August 2014.

References II

- Michael T. Goodrich and Roberto Tamassia.
  Introduction to Computer Security.
  Pearson, 2011.

- Thomas W. Judson.
  Abstract Algebra.
  Orthogonal Publishing, L3C, 2016.

- Bruce Schneier.
  Applied Cryptography.
  John Wiley & Sons, Inc, 1996.

- Simon Singh.
  The Code Book.
  Anchor Books, 1999.