ISC
(BTech III Jan-April 2024)
## Week#5 – Feb 2, 2024

Dhiren Patel

Polygram substitution

- Groups of characters being substituted (simultaneously) by other groups of characters from the same alphabet
- Sequences of two plaintext characters (*digrams*) be replaced by other digrams;
- key space is large
- Applicable to trigrams to n-grams

Polygram ciphers (attacks)

- polygram substitution ciphers (Playfair, Hill) are linear transformation, and fall under known-plaintext attack.

- Frequency analysis (digrams)
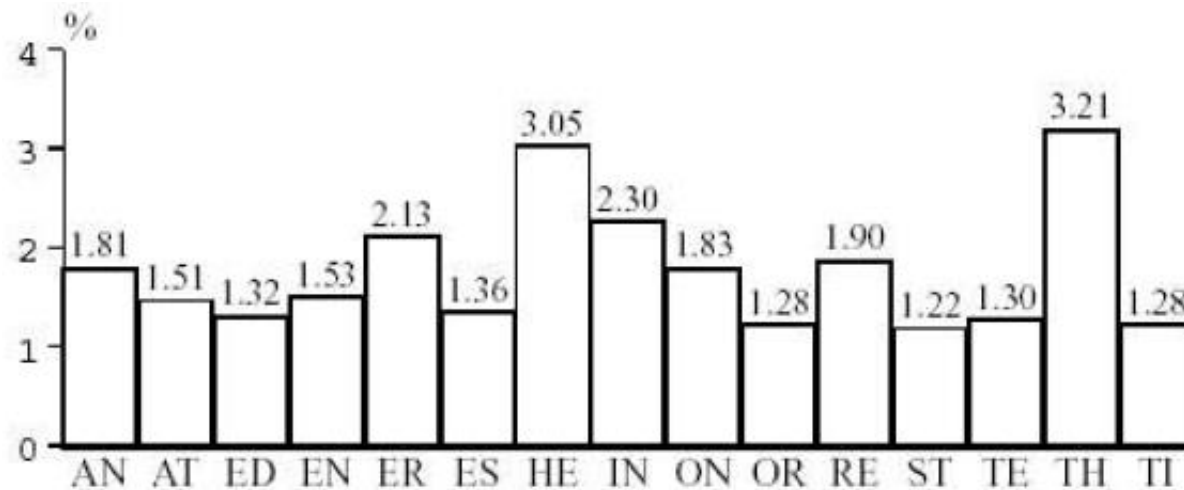
Similarly -- Trigrams - The most common trigrams (triples) in English language are: THE, ING, AND, HER, ERE, ENT, THA and NTH.

Poly-alphabetic substitutions

- letters of plain text are mapped into letters of cipher text space <u>depending on their position</u> in the text
- the same plaintext character is thus encrypted to different ciphertext characters, resisting simple frequency analysis of mono-alphabetic substitution

Poly-alphabetic substitution

- Key is taken from some known text (with corresponding character value (0 to 25)) defining the shifting of underlying m.

- The mapping of plaintext $m = m_1\ m_2\ m_3\ ...$ to ciphertext $\boldsymbol{c} = c_1\ c_2\ c_3\ ...$ is defined on individual characters by $c_i = (m_i + k_i)$ mod s, where subscript $\boldsymbol{i}$ in k_i is taken modulo t (the key is re-used)

Vigenère cipher - Vigenère table

- Blaise de Vigenère (French diplomat, translator, cryptographer – 1523-1596)
- the Each of the 26 shift ciphers is laid out horizontally, with the key letter for each cipher to its left.
- Plain text runs across the top.
- The cipher text is at the intersection of the row labeled key letter "k" and the column labeled text letter "p".
- Eg. Plain text "baby" – encrypted using key "abcd" → bbdb

	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

- a method of encrypting alphabetic text where each letter of the plaintext is encoded with a different Caesar cipher, whose increment is determined by the corresponding letter of another text, the key

Vigenère cipher

- To encrypt a message, a key is needed that is as long as the message. Usually the key is a repeating keyword.

- To decrypt the cipher text, the key letter again defines the row, and the position of ciphertext letter in that row determines the column. The top letter on that column is decrypted letter.

- E.g. *Plain text*: Meet at five pm behind P lab.

- *Keyword phrase*: confidential

Plain text	m	e	e	t	a	t	f	i	v	e	p	m	b	e	h	i	n	d	p	l	a	b
Key	c	o	n	f	i	d	e	n	t	i	a	l	c	o	n	f	i	d	e	n	t	i
Cipher text	o	s	r	y	i	w	j	v	o	m	p	x	d	s	u	n	v	g	t	y	t	j
Recovered	m	e	e	t	a	t	f	i	v	e	p	m	b	e	h	i	n	d	p	l	a	b

Breaking Vigenère cipher

- The cryptanalyst looking only at the ciphertext would detect the repeated sequences of common digrams and trigrams, devise common factors in the displacements of the various sequences, and make good guess of the keyword length.

- If the keyword is of length N, then the cipher is consisting N mono-alphabetic substitution ciphers.

- One can use the known frequency characteristics of a plain text language to attack each of the mono-alphabetic ciphers separately.

- Refinement leads to eliminate periodic nature of the keyword (very long keyword would help).

Vigenère cipher

- Running-key *Vigenère*

  If the key stream k_i of a simple *Vigenère* is as long as the plaintext, the cipher is called a *running-key cipher*. For example, the key may be meaningful text from a known book (properly synchronized).

- If the key has redundancy – cryptanalyst can exploit statistical imbalances;

- E.g., when encrypting plaintext English characters using a meaningful text as a running key, cryptanalysis is possible based on the observation that a significant proportion of ciphertext characters results from the encryption of high-frequency running text characters with high-frequency plaintext characters. (unigram frequency analysis)

Vernam Cipher

- The system can be expressed as:

$c_i = m_i \oplus k_i$ – Encryption

$m_i = c_i \oplus k_i$ – Decryption

- where, $m_i = i^{\text{th}}$ binary digit of plain text
- $k_i = i^{\text{th}}$ binary digit of key material
- $c_i = i^{\text{th}}$ binary digit of cipher text
- $\oplus$ = exclusive-or (XOR) operation

Gilbert Vernam in 1918 proposed the use of a running tape that eventually repeated the key, so that the system can work with a very long (but repeating) keyword.

One-time pad – unbreakable cipher!

- A one-time pad (OTP) is a large non-repeating set of random key letters, written on sheets of paper, and glued together in a pad.

- The sender uses each key letter on the pad to encrypt exactly one plaintext character. (*Major Joseph Mauborgne* - an Army Signal Corp officer)

- The sender encrypts the message and then destroys the used pages of the pad.

- The receiver has an identical pad and uses each letter on the pad, in turn, to decrypt each letter of the cipher-text. The receiver destroys the same used pages of the pad after decrypting the message.

OTP - Vernam

- This idea can be easily extended to binary data by using a one-time pad of key bits and XOR operation (same as Vernam cipher – with non repeating random key).

- To decrypt, XOR the cipher-text with a string from an equivalent copy of the one-time pad. Everything else remains the same and security is just as perfect as there are no patterns or regularities that a cryptanalyst can use to attack.

- Problems associated with key generation (truly random), key distribution, and perfect synchronization between the sender and receiver(s).

Security of One Time Pad

- A random key sequence "added" to a nonrandom plaintext message produces a completely random cipher-text message and no amount of computing power can break that.

- Conditional security v/s un-conditional security

- Two time pad – Same key used twice!

Lab next two weeks

- Implement Vigenere cipher – with repeating keyword
- Implement Vigenere cipher – with running key (key is as long as plaintext)
- Vigenere cipher is essentially multiple Caesar ciphers!!
- Implement One time pad (Key generation using good RNG, Key directory, Encrypt (output in hexadecimal format), Decrypt)

RSAC 2024 San Francisco May 2024
Shaping Tomorrow's Cybersecurity Landscape

1 COMMUNITY MATTERS
Explore collaboration, mental health, and securing our digital world.

2 HUMANS AND TECHNOLOGY
Discover new perspectives in cybersecurity emphasizing collaboration to address human-related risks effectively.

3 LEGISLATION & POLICY
Discover the influence of global legislation on cybersecurity, prompting reassessment of compliance and risk management.

4 AI & EVERYTHING
Explore diverse AI applications, ethical considerations, and practical insights into opportunities and responsibilities in AI integration.

5 SECURE BY DESIGN
Delve into OWASP strategies, threat modeling, and secure code practices.

RSAC 2024 San Francisco May 2024 Themes

6 **THREAT MODELING**
Master threat modeling by navigating adoption challenges, integrating threat intelligence, exploring business value, and applying it to understand human behavior.

7 **A PRIVACY-FIRST MINDSET**
Navigate comprehensive attack frameworks and adeptly employ privacy methods for enhanced cybersecurity.

8 **RANSOMWARE RISES AGAIN**
Explore the resurgence of ransomware, with predictions reaching $900 million, emphasizing the urgency to fortify cybersecurity.

9 **TELECOMMUNICATIONS & SECURITY**
Dive into the security challenges faced by telecommunications amid rising attacks and the 5G to 6G transition.

10 **SECURITY'S IDENTITY SHIELD**
Addressing the essential necessity to bridge the gap between identity and security teams.

Webinar – Feb 15 - Triple Extortion

- With the triple extortion approach, attackers aim to compel victims into paying multiple ransoms by introducing extra threats and risks beyond just blocking access to data.

Ransomware and Double extortion

- In a traditional ransomware attack, an attacker encrypts and locks the victim from accessing their data.

- In a double extortion ransomware attack, a second attack vector -- exfiltrating data to expose -- is added.

- Victim organizations can often recover from a traditional ransomware attack using backups.

- By exfiltrating data in a double extortion attack, the attacker has another chance to extort the victim -- or demand two ransoms.

- Attackers can threaten to publish, leak or sell the stolen data on the dark web if a second ransom isn't paid.

Triple extortion

- third attack vector could be a distributed denial-of-service (DDoS) attack or intimidation of the victim's customers, employees and stakeholders into paying a ransom.

Triple extortion ransomware attack

Lateral movement · Data encryption · Payment or recovery · Ransom demand · DDoS attack · Payment or recovery

Initial access · Data exfiltration · Ransom demand · Threaten data leak · Payment or recovery · Ransom demand

Traditional ransomware	Double extortion ransomware	Triple extortion ransomware
Encrypts files on the victim's system.	Encrypts files on the victim's system.	Encrypts files on the victim's system.
	Exfiltrates data and threatens to publish or leak it if the ransom isn't paid.	Exfiltrates data and threatens to publish or leak it if the ransom isn't paid.
		Threatens to disrupt the victim organization's operations through attacks, such as a DDoS, if the ransom isn't paid. Attackers sometimes opt to seek a ransom payment by threatening the victim's customers, employees and stakeholders.

How does a triple extortion ransomware attack work?

- At the initial stages, a triple extortion ransomware attack follows the same basic attack sequence as a common ransomware attack but adds the second and third attack vectors. A typical triple extortion ransomware attack has the following steps:

1.**Initial access.** Attackers gain entry into their victim's network, often through phishing, malware, vulnerabilities or stolen credentials.

2.**Lateral movement and asset discovery.** Once they have access to the network, attackers probe deeper into an environment to elevate privileges and find potentially valuable data.

How does a triple extortion ransomware attack work?

3. **Data exfiltration.** Once identified, high-value assets are stolen to use in a double extortion attack.

4. **Encryption of files.** Attackers encrypt the data to prevent the victim from accessing it.

5. **Ransom demand.** With the data encrypted and exfiltrated, attackers send a ransom note to the victim demanding payment, typically in a <u>cryptocurrency</u>, to receive the decryption key and regain access.

How does a triple extortion ransomware attack work?

6. **Double extortion ransom demand.** If the victim organization is able to restore its data from backups -- or even if it paid the first ransom -- the malicious actors return for a second attack and demand a second ransom payment to prevent them from publishing or leaking the victim's sensitive data.

7. **Triple extortion ransom demand.** In the third attack, attackers threaten additional exploitation, such as a DDoS attack or even approaching the victim organization's customers, employees and third parties to demand a payment.

Examples

- **BlackCat.**

- Also known as ALPHV, the BlackCat ransomware group became a major threat in 2022 with attacks against fuel and aviation companies, as well as universities.

- In 2023, the group claimed responsibility for the cyber attack on <u>Barts Health NHS Trust</u>.

Examples

- **Hive.** The Hive ransomware group executed large triple extortion ransomware attacks until late 2022 when U.S. law enforcement disrupted its operations.

- **Vice Society.** In 2022 and 2023, Vice Society emerged as a triple extortion ransomware threat, targeting public sector and educational organizations. In February 2023, Vice Society claimed it had successfully attacked the San Francisco Bay Area Rapid Transit system.