ISC

(BTech III Jan-April 2024)
Week#2 – Jan 12, 2024

Dhiren Patel

How do we check meaningful output while automating a brute force attack on Caesar cipher?

- Compare Decrypted Words to a Dictionary:
- For each attempted shift, count the number of words in the decrypted text that appear in a standard English dictionary.
- The shift that yields the highest number of valid words is likely the correct one.
- Utilize a Word Frequency List:
- Compare the frequency of words in the decrypted text to known word frequencies in the English language.
- The shift that produces the most common words in their expected proportions is likely the correct one.
- Examples are “is”, “are”, “the”, “hi”

How do we check meaningful output while automating a brute force attack on Caesar cipher?

- Contextual Clues:
- Consider Known Information:
- If you have any information about the message's context (e.g., sender, topic), use it to assess the likelihood of different decryption results.
- For example, if you know the message is about sports, a decryption that contains sports-related words is more likely to be correct.
- (Human judgment can often identify meaningful text that automated techniques might miss.)
- E.g. Contexts - Vibrant Gujarat, Surat as the Cleanest city, Cricket Worldcup


Malware
Threats against data
Social Engineering threats
Information Manipulation
ENISA THREAT LANDSCAPE
Supply-chain attacks
Ransomware
Threats against availability: Denial of Service
Threats against availability: Internet threats

Key definitions – cont. from the last week

- Social engineering attacks encompasses a broad range of activities that attempt to exploit human error or human behaviour with the objective of gaining access to information or services. It uses various forms of manipulation to trick victims into making mistakes or handing over sensitive or secret information.
- Users may be lured to open documents, files or e-mails, to visit websites or to grant access to systems or services. Although the lures and tricks used may abuse technology, they rely on a human element to be successful.
- While social engineering techniques are often used to gain initial access, they may also be used at later stages in an incident or breach. Notable examples are business e-mail compromise, fraud, impersonation, counterfeit and, more recently, extortion.

Threats against the data can be classified into :
1.Data breach
2.Data leak

Key definitions

- A data breach is defined as any breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed (Ref: GDPR)
- Technically speaking, threats against data can be mainly classified as data breach or data leak.
- Data breach is an intentional cyber-attack brought by a cybercriminal with the goal of gaining to unauthorized access and release sensitive, confidential or protected data.
- Data leak is an event (e.g. misconfigurations, vulnerabilities or human errors) that can cause the unintentional loss or exposure of sensitive, confidential or protected data.

Data leak => It is caused due to the unintentional loss or exposure of sensitive data, confidential data or protected data.

Key definitions

- Availability Attacks (Denial of Service) - occur when users of a system or service are not able to access relevant data, services or other resources.
- This can be accomplished by exhausting the service and its resources or overloading the components of the network infrastructure.
- DoS attacks are most easy to launch and to occur!!! (E.g. Result website)
- Threats to Internet availability refer to intentional or unintentional disruptions of Internet or electronic communications that result in Internet outages, blackouts, shutdowns or censorship.
- Internet disruptions can be due to government-directed Internet shutdowns, cyclones, massive earthquakes, power outages, cable cuts, cyberattacks, technical problems and military actions.

Threats to the Internet availability is to refer to intentional or unintentional disruptions of the Internet or electronic communications... that would result into cobs(censorship, ownership, blackouts, shutdowns).

Discussion

Internet disruptions kyare thai sake 6e??
due to government-directed Internet ...
shutdowns, cyclones, massive earthquakes, power outages,
cable cuts , cyberattacks, technical problems, and military actions.

- Peer Learning
- Better TLR – Teaching, Learning and Research
- Curriculum and Rigor
- Too many courses?
- Internships and Employment offer
- Screen Time and Social Network Profile
- Privacy and Rights
- Fake identities and Proof of Personhood

Classical Ciphers

- *classical ciphers* -- illustrate important basic principles and common pitfalls
- Ciphers are further classified as:
- *Mono-alphabetic* - only one substitution/ transposition is used
- *Poly-alphabetic* - where several substitutions/ transpositions are used
- several such ciphers may be concatenated together to form a *product cipher*
- Steganography (hiding / concealing information)
- Machine ciphers (Rotor machines)

Transposition Cipher – Example 1 (Rail fence)

- Text is written down as a sequence of diagonals (Rail fence) and then read of as a sequence of rows.
- *Plain text*: Meet at five pm behind P lab.
- Written as *Rail fence* of depth 2:

m		e		a		f		v		p		b		h		n		p		a	
	e		t		t		i		e		m		e		i		d		l		b

- Encrypted as: meafvpbhnpa ettiemeidlb
- Where to cut the halves? (message length should be even, append x at the end; if required)

Transposition cipher - example 2 (Permutation)

- a simple transposition with t = 6 and e = (6 4 1 3 5 2) as a *permutation* on the set.
- The message m = CAESAR is encrypted to c = RSCEAA.
- Decryption uses the inverse permutation d = (3 6 4 2 5 1).
- A mnemonic keyword may be used in place of a key. For example, for n = 6, the keyword "CIPHER" could be used to specify the column ordering 1, 4, 5, 3, 2, 6 (by alphabetic priority).
- Sequential composition of two or more simple transpositions with respective periods t_1, t_2, … , t_i is called a *compound transposition*.

Transposition cipher – example 3 (columnar)

- write a message in a rectangle (square matrix), row by row and read it off, column by column.
- Plain text message: meet at five pm behind p lab

m	e	e	t	a
t	f	i	v	e
p	m	b	e	h
i	n	d	p	l
a	b	x	x	x

- Encrypted text (5x5 matrix): <read column vise>
- mtpia efmnb eibdx tvepx aehlx
- xxx is appended to make message 25 character long.
- Block size (matrix size and dimension)

Transposition cipher (Cont.)

- Additionally, a key can also be defined to permute the order of the columns. Write text in a row by row..

mtpia efmnb eibdx tvepx aehlx

m	e	e	t	a
t	f	i	v	e
p	m	b	e	h
i	n	d	p	l
a	b	x	x	x

- E.g. key (41523) defines -- read it off – 4th column first, 1st column second, 5th column third, followed by 2nd and 3rd column, and prepare encrypted text.
- Encrypted text is:
- tvepx mtpia aehlx efmnb eibdx

Lab next week – Classical Cryptography

- Transposition ciphers – implement both Encryption and Decryption
- Plain text – original msg (readable text)
- Cipher text – transformed msg (encrypted)
- Rail Fence Cipher (depth 2 and depth 3),
- Permutation cipher (period (block size) up to 10) – how to compute reverse permutation?,
- Columnar cipher (5x5) with column ordering,