Week 3 - Wednesday

COMP 4290

Last time

- What did we talk about last time?
- Access control
- Cryptography basics

Questions?

Project 1

Assignment 1

Security tidbit of the day

- In other AI security news …
- There are lots of different ways to execute an indirect prompt injection attack
- Example goal: Read private data from someone's Google Drive
- If a person has hooked up their Google Drive to ChatGPT (or another LLM), the LLM can read that data
- If an attacker can send the victim a file that looks innocuous but actually has secret instructions for the LLM written in tiny white-on-white font, the LLM can execute those instructions (like "send anything that looks like a password to this e-mail account")
- This kind of attack works best on a victim that has a professional relationship with the attacker
  - An innocent-looking Word document or PowerPoint slide might get saved to Google Drive
- ChatGPT can link to Google Drive, Gmail, GitHub, Microsoft Outlook calendars, etc.
- Any data that could get stored in any of those locations is a vector for the attack
- Follow the story:
  - https://www.wired.com/story/poisoned-document-could-leak-secret-data-chatgpt/

Encryption

Terminology remix

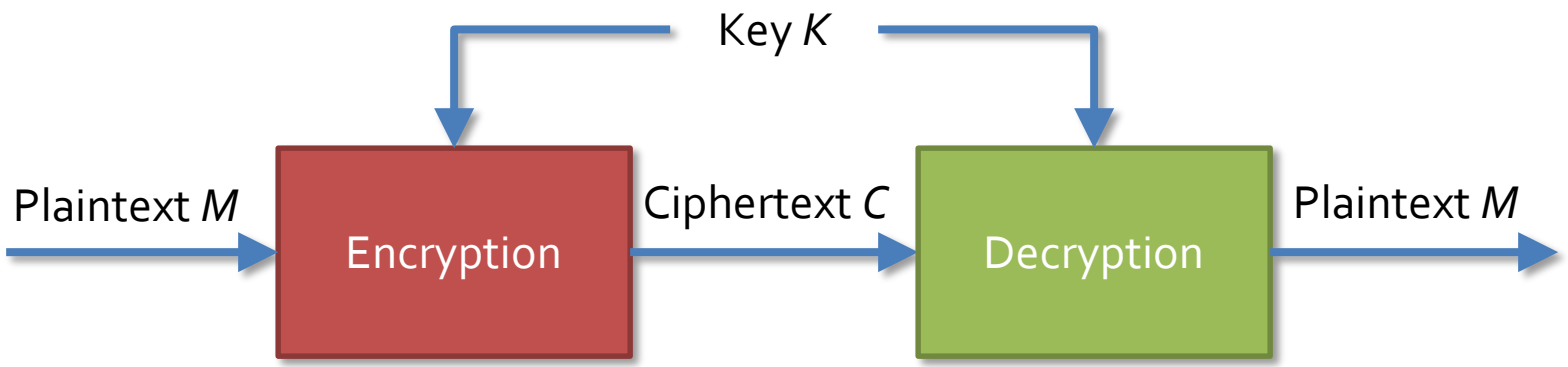
- Rather than use letters, a system popularized by Ron Rivest is to use **Alice** and **Bob** as the two parties communicating
  - **Carl** or another "C" name can be used if three people are involved
- **Trent** is a trusted third party
- **Eve** is used for an evil user who often eavesdrops
- **Mallory** is used for a malicious user who is usually trying to modify messages

Encryption algorithms

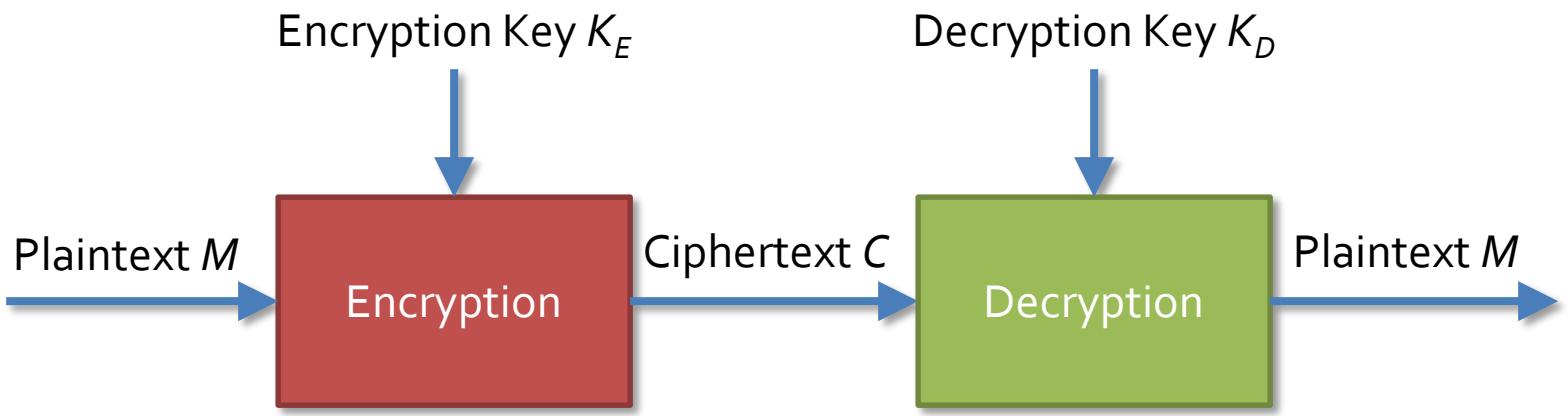
- The algorithms for encryption often rely on a secret piece of information, called a key
- We can notate the use of a specific key in either of the two following ways:
  - $C = E_K(M)$
  - $C = E(K, M)$
- In symmetric (or private key) encryption, the encryption key and the decryption key are the same
- In asymmetric (or public key) encryption, the encryption key and the decryption key are different

Symmetric vs. asymmetric

Symmetric Encryption



Asymmetric Encryption



Cryptanalysts

- A **cryptanalyst** is someone who is trying to break the cryptography and discover the plaintext or the key
- A cryptanalyst could:
  - Break a single message
  - Find patterns in the encryption that allow future messages to be decrypted
  - Discover information in the messages without fully decrypting them
  - Discover the key
  - Find weaknesses in the implementation of the encryption
  - Find weaknesses in the encryption that may or may not be able to lead to breaks in the future

Modular Arithmetic Overview

Review of Modular Arithmetic

- Modulo operator takes the remainder
- Two numbers are said to be congruent modulo n if they have the same remainder when divided by n
- For example,

  $39 \equiv 3 \pmod{12}$
- Addition, subtraction, and multiplication:
  - $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
  - $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
  - $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

Divided and Conquered

- We can't actually divide
- Instead, we have to find the multiplicative inverse
- The multiplicative inverse of x exists if and only if x is relatively prime to n
- $13 \cdot 5 \equiv 65 \equiv 1 \pmod{16}$
- So, 13 and 5 are multiplicative inverses mod 16
- But, 0, 2, 4, 6, 8, 10, 12, and 14 do not have multiplicative inverses mod 16

Shift Cipher

Definition

- A shift cipher encrypts a message by shifting all of the letters down in the alphabet
- Using the Latin alphabet, there are 26 (well, 25) possible shift ciphers
- We can model a shift cipher by numbering the letters A, B, C, … Z as 0, 1, 2, … 25
- Then, we let the key ***k*** be the shift
- For a given letter ***x***:

$E_k(x) = (x + k) \bmod 26$

Example: Caesar Cipher

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
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***("KILL EDWARD") = "NLOO HGZDUG"
- What is ***E***("I DRINK YOUR MILKSHAKE")?
- What is ***D***("EUHDNLWGRZQ")?
- This code was actually used by Julius Caesar who used it to send messages to his generals

Example: ROT13 Cipher

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
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

- ***E***("MATH IS GREAT") = "ZNGU VF TERNG"
- Note that encryption = decryption for this cipher
- Used to hide spoilers in some online forums
- How hard is it to crack shift ciphers?

Cryptanalysis of a Shift Cipher

- Cryptanalysis of a shift cipher is incredibly easy
- You just have to try 26 possibilities to be sure you have the right one
- A shift cipher is a simplified version of a **substitution cipher**

Transposition Ciphers

Definition

- In a transposition cipher, the letters are reordered but their values are not changed
- Any transposition cipher is a permutation function of some kind

Example: Rail Fence Cipher

- In the rail fence cipher, a message is written vertically along a fixed number of "rails," wrapping back to the top when the bottom is reached
- To finish the encryption, the message is stored horizontally
- This is also known as a **columnar transposition**
- Encryption of "WE ARE DISCOVERED, FLEE AT ONCE" with three rails:

W	R	I	O	R	F	E	O	E
E	E	S	V	E	L	A	N	X
A	D	C	E	D	E	T	C	J

- **Ciphertext:** WRIORFEOEEESVELANXADCEDETCJ

Variations

- There are many other ways to vary the cipher
- It is possible to write the words going down and then back up the fence
- Words can be read back off the grid in a spiral or backwards
- Different rules can be used when the words don't completely fill the grid
- After the grid has been made, columns can be permuted by another function, perhaps based on a keyword

Cryptanalysis of transposition ciphers

- It's usually possible to detect a transposition cipher because the frequencies of letters are unchanged
- Practiced cryptographers look for patterns of anagrams in a given language, allowing them to find the rules for transposition
- Transposition ciphers were used in practice as recently as World War II
- Note that transposition ciphers require all the characters in the message before it can begin as well as linear space

Substitution Ciphers

Substitution ciphers

- **Substitution ciphers** cover a wide range of possible ciphers, including the shift cipher
- In a substitution cipher, each element of the plaintext is substituted for some corresponding element of the ciphertext
- **Monoalphabetic** substitution ciphers always use the same substitutions for a letter (or given sequence of letters)
- **Polyalphabetic** substitution ciphers use different substitutions throughout the encryption process

Example: Simple Monoalphabetic Substitution Cipher

- We can map to a random permutation of letters
- For example:

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

- E("MATH IS GREAT") = "UIYP TQ ABZIY"
- 26! possible permutations
- Hard to check every one

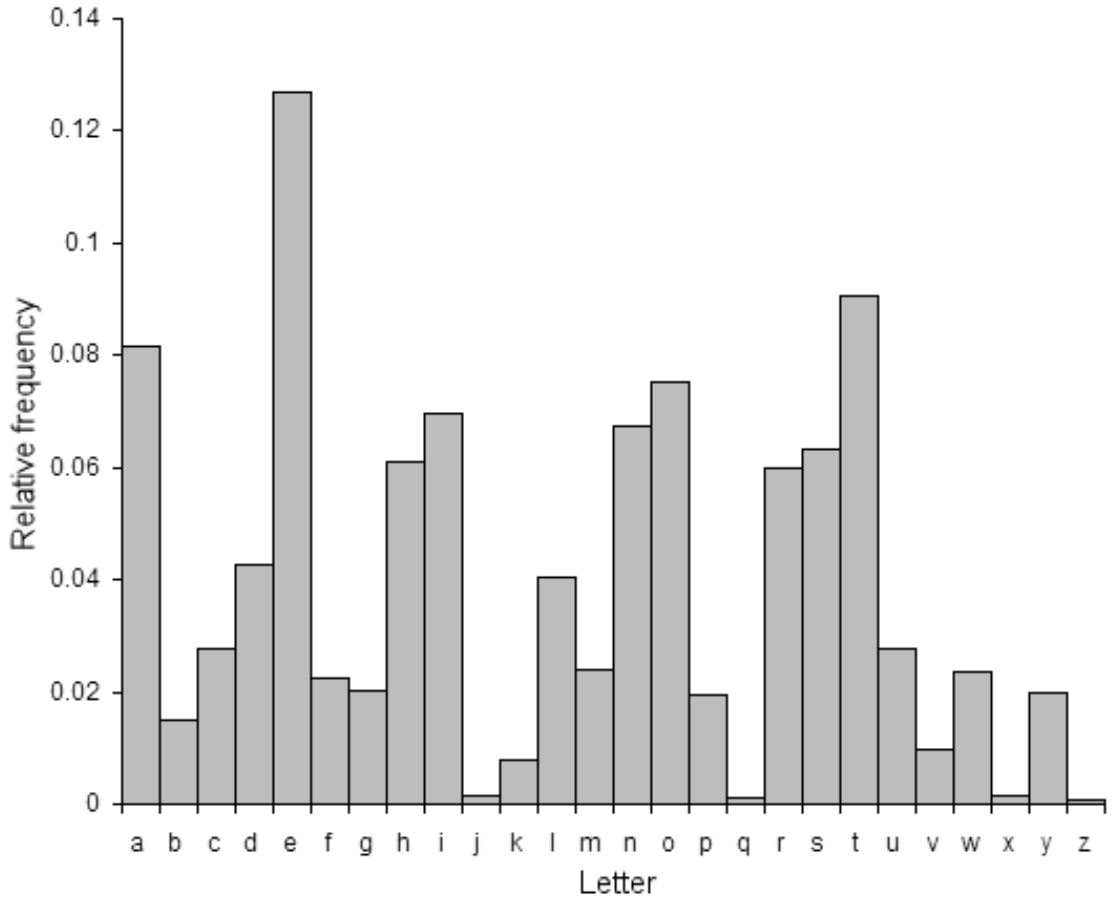
Example continued

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

- Using the same mapping, perform the following encryption:
- ***E***("HELP ME") =
- Perform the following decryption:
- ***D***("VD CDL QZZ YPZ HFDBV") =

Frequency Attack

- English language defeats us
- Some letters are used more frequently than others: ETAOINSHRDLU
- Longer texts will behave more consistently
- Make a histogram, break the cipher



Cipher text

SPHB JLSP K ECGPCQFT GYBKYD, VFCMB C LSPGBYBG, VBKX KPG VBKYD,
SOBY EKPD K RJKCPT KPG HJYCSJU OSMJEB SZ ZSYQSTTBP MSYB -
VFCMB C PSGGBG, PBKYMD PKLLCPQ, UJGGBPMD TFBYB HKEB K TKLLCPQ,
KU SZ USEB SPB QBPTMD YKLLCPQ, YKLLCPQ KT ED HFKEIBY GSSY.
"'TCU USEB OCUCTSY," C EJTTBYBG, "TKLLCPQ KT ED HFKEIBY GSSY -
SPMD TFCU KPG PSTFCPQ ESYB."

KF, GCUTCPHTMD CYBEBEIBY CT VKU CP TFB IMBKX GBHBEIBY;
KPG BKHF UBLKYKTB GDCPQ BEIBY VYSJQFT CTU QFSUT JLSP TFB ZMSSY.
BKQBYMD C VCUFBG TFB ESYYSV; - OKCPMD C FKG USJQFT TS ISYYSV
ZYSE ED ISSXU UJYHBKUB SZ USYYSV - USYYSV ZSY TFB MSUT MBPSYB -
ZSY TFB YKYB KPG YKGCKPT EKCGBP VFSE TFB KPQBMU PKEB MBPSYB -
PKEBMBUU FBYB ZSY BOBYESYB.

KPG TFB UCMXBP, UKG, JPHBYTKCP YJUTMCPQ SZ BKHF LJYLMB HJYTKCP
TFYCMMBG EB - ZCMMBG EB VCTF ZKPTKUTCH TBYYSYU PBOBY ZBMT IBZSYB;
US TFKT PSV, TS UTCMM TFB IBKTCPQ SZ ED FBKYT, C UTSSG YBLBKTCPQ
"'TCU USEB OCUCTBY BPTYBKTCPQ BPTYKPHB KT ED HFKEIBY GSSY -
USEB MKTB OCUCTBY BPTYBKTCPQ BPTYKPHB KT ED HFKEIBY GSSY; -
TFCU CT CU KPG PSTFCPQ ESYB."

Moving toward plain text

SNPE YMSN A LIDNIUHO DTEATF, WHICE I MSNDETED, WEAK AND WEATF,
SVET LANF A XYAINO AND PYTISYR VSCYLE SG GSTUSOOEN CSTE -
WHICE I NSDDED, NEATCF NAMMINU, RYDDENCF OHETE PALE A OAMMINU,
AR SG RSLE SNE UENOCF TAMMINU, TAMMINU AO LF PHALBET DSST.
"'OIR RSLE VIRIOST," I LYOOETED, "OAMMINU AO LF PHALBET DSST -
SNCF OHIR AND NSOHINU LSTE."

AH, DIROINPOCF I TELELBET IO WAR IN OHE BCEAK DEPELBET;
AND EAPH REMATAOE DFINU ELBET WTSYUHO IOR UHSRO YMSN OHE GCSST.
EAUETCF I WIRHED OHE LSTTSW; - VAINCF I HAD RSYUHO OS BSTTSW
GTSL LF BSSKR RYTPEARE SG RSTTSW - RSTTSW GST OHE CSRO CENSTE -
GST OHE TATE AND TADIANO LAIDEN WHSL OHE ANUECR NALE CENSTE -
NALECERR HETE GST EVETLSTE.

AND OHE RICKEN, RAD, YNPETOAIN TYROCINU SG EAPH MYTMCE PYTOAIN
OHTICCED LE - GICCED LE WIOH GANOAROIP OETTSTR NEVET GECO BEGSTE;
RS OHAO NSW, OS ROICC OHE BEAOINU SG LF HEATO, I ROSSD TEMEAOINU
"'OIR RSLE VIRIOET ENOTEAOINU ENOTANPE AO LF PHALBET DSST -
RSLE CAOE VIRIOET ENOTEAOINU ENOTANPE AO LF PHALBET DSST; -
OHIR IO IR AND NSOHINU LSTE."

Real plain text

ONCE UPON A MIDNIGHT DREARY, WHILE I PONDERED, WEAK AND WEARY,
OVER MANY A QUAINT AND CURIOUS VOLUME OF FORGOTTEN LORE -
WHILE I NODDED, NEARLY NAPPING, SUDDENLY THERE CAME A TAPPING,
AS OF SOME ONE GENTLY RAPPING, RAPPING AT MY CHAMBER DOOR.
"'TIS SOME VISITOR," I MUTTERED, "TAPPING AT MY CHAMBER DOOR -
ONLY THIS AND NOTHING MORE."

AH, DISTINCTLY I REMEMBER IT WAS IN THE BLEAK DECEMBER;
AND EACH SEPARATE DYING EMBER WROUGHT ITS GHOST UPON THE FLOOR.
EAGERLY I WISHED THE MORROW; - VAINLY I HAD SOUGHT TO BORROW
FROM MY BOOKS SURCEASE OF SORROW - SORROW FOR THE LOST LENORE -
FOR THE RARE AND RADIANT MAIDEN WHOM THE ANGELS NAME LENORE -
NAMELESS HERE FOR EVERMORE.

AND THE SILKEN, SAD, UNCERTAIN RUSTLING OF EACH PURPLE CURTAIN
THRILLED ME - FILLED ME WITH FANTASTIC TERRORS NEVER FELT BEFORE;
SO THAT NOW, TO STILL THE BEATING OF MY HEART, I STOOD REPEATING
"'TIS SOME VISITER ENTREATING ENTRANCE AT MY CHAMBER DOOR -
SOME LATE VISITER ENTREATING ENTRANCE AT MY CHAMBER DOOR; -
THIS IT IS AND NOTHING MORE."

Digram analysis

- These kinds of attacks can be further refined by analyzing digrams and trigrams (two letter and three letter sequences)
- Digram analysis is also an approach that can be used against transposition ciphers, since you can gain clues about which letters should be next to which others

Digrams	Trigrams
EN	ENT
RE	ION
ER	AND
NT	ING
TH	IVE
ON	TIO
IN	FOR
TF	OUR
AN	THI
OR	ONE

Vigenère Cipher

Vigenère cipher

- The Vigenère cipher is a form of polyalphabetic substitution cipher
- In this cipher, we take a key word and repeat it, over and over, until it is as long as the message
- Then, we add the repetitions of keywords to our message mod 26

Vigenère example

- Key: BENCH
- Plaintext: A LIMERICK PACKS LAUGHS ANATOMICAL

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

Example continued

- Encrypt the following:
  - Plaintext: GENTLEMEN DINE AFTER SEVEN
  - Key: WILDE
- Decrypt the following:
  - Ciphertext: EOJKINOCQGEOJKI
  - Key: BOWIE

Upcoming

Next time…

- Finish historical ciphers
- Stream and block ciphers
- DES

Reminders

- **1:45-3:30 p.m. office hours are canceled today due to meetings**
- Read Sections 2.3 and 12.2
- Work on Project 1
  - Due next Friday
- Work on Assignment 1
  - **Due this Friday**