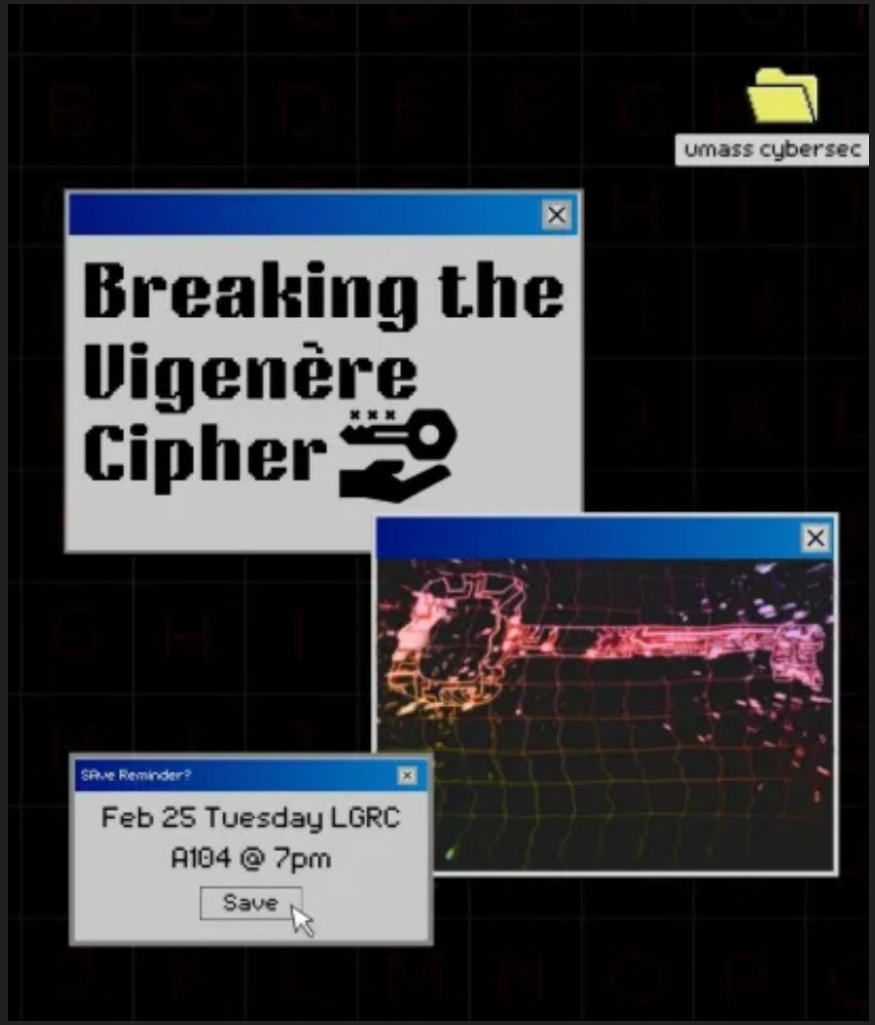
Breaking the Vigenère Cipher

An Introduction to Cryptography



UMASS CYBERSEC CLUB

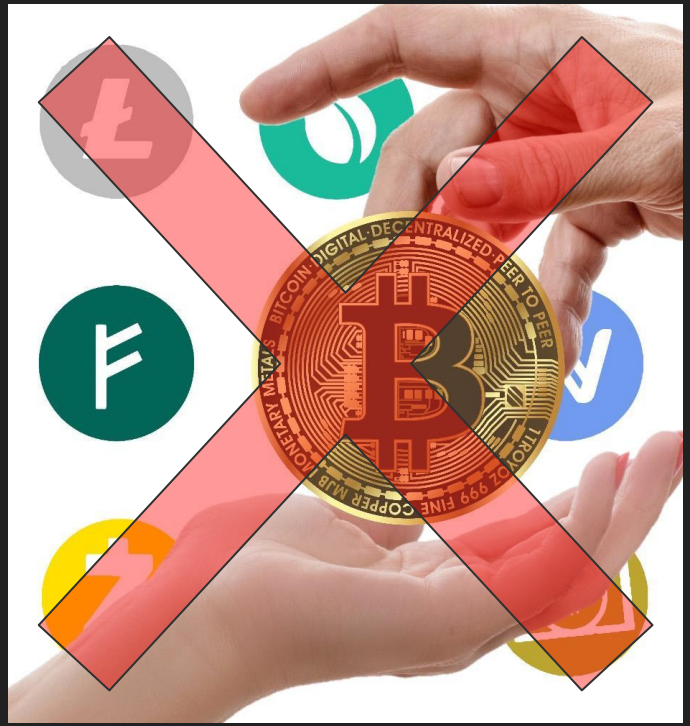
What is Cryptography?

- Sharing secret messages with math
- Primarily used to keep your internet traffic safe
- Some common encryption standards
  - RSA
  - AES
- **Encryption** should be easy to do, but **decryption** should be hard
- We will examine and break two **ciphers** today
  - Caesar
  - Vigenère

UMASS CYBERSEC CLUB

What is Cryptography?

- Sharing secret messages with math
- Primarily used to keep your internet traffic safe
- Some common encryption standards
  - RSA
  - AES
- **Encryption** should be easy to do, but **decryption** should be hard
- We will examine and break two **ciphers** today
  - Caesar
  - Vigenère



UMASS CYBERSEC CLUB

Atbash Cipher

UMass Amherst => FNzhh Znsvihg

FNzhh Znsvihg => UMass Amherst

this is a problematic cipher => gsrh rh z kilyovnzgrx xrksvi

Atbash Cipher

UMass Amherst => FNzhh Znsvihg

FNzhh Znsvihg => UMass Amherst

this is a problematic cipher => gsrh rh z kilyovnzgrx xrksvi

Letter in **plaintext**:	`abcdefghijklmnopqrstuvwxyz`
Letter in **ciphertext:**	`zyxwvutsrqponmlkjihgfedcba`

The Game

- Alice wants to send a message to Bob, but Eve is listening in
- How can they get around this?

UMASS CYBERSEC CLUB

The Game

- Alice wants to send a message to Bob, but Eve is listening in
- How can they get around this?
  - Alice can garble the text in some way that Bob can undo it
    - Atbash Cipher! Swap every letter with its opposite, a with z, b with y...
    - But Eve can immediately figure it out

UMASS CYBERSEC CLUB

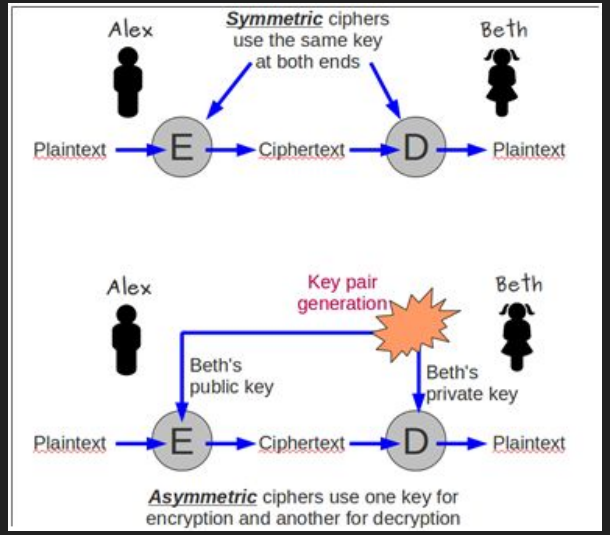
The Game

- Alice wants to send a message to Bob, but Eve is listening in
- How can they get around this?
  - Alice can garble the text in some way that Bob can undo it
    - Atbash Cipher! Swap every letter with its opposite, a with z, b with y...
    - But Eve can immediately figure it out
  - Alice tells Bob a secret **key** to add complexity to the message
    - This is a key idea in modern cryptography

UMASS CYBERSEC CLUB

More on Keys

- A value that helps us secure messages
- Symmetric key encryption
  - Used in most ciphers and AES
  - Same key for encrypting and decrypting
  - Shared secretly before communication
- Asymmetric key encryption
  - Used in RSA and Diffie-Hellman Key Exchange
  - Alice makes a pair of keys
  - Public key used to send encrypted messages to Alice
  - Alice keeps private key to decrypt messages
  - Public key is like a “lock”
  - Anyone can put a lock on their message, but only Alice can decrypt it



UMASS CYBERSEC CLUB

Caesar Cipher

- Used by Caesar to communicate with his officers
- The key is a “shift”
- We apply the shift to each letter to encrypt it
- We shift each letter backwards by our key to decrypt
- Let’s try an example!

UMASS CYBERSEC CLUB

Encrypt Caesar Cipher Example

- Handy wheels invented after Caesar let us encrypt and decrypt quickly
- From the outer wheel to the inner wheel
- Shift = 17 (a ➜ r, b ➜ s, ...)
- Non-alphabetic characters?

plaintext	q	u	i	c	k		b	r	o	w	n
ciphertext											

UMASS CYBERSEC CLUB

Encrypt Caesar Cipher Example

- Handy wheels invented after Caesar let us encrypt and decrypt quickly
- From the outer wheel to the inner wheel
- Shift = 17 (a ➜ r, b ➜ s, ...)
- Non-alphabetic characters?

plaintext	q	u	i	c	k		b	r	o	w	n
ciphertext	h	l	z	t	b		s	i	f	n	e

UMASS CYBERSEC CLUB

Decrypt Caesar Cipher Example

- To undo Caesar Cipher, we shift again
- Go from the inner wheel to the outer wheel
- To undo a shift of +17, we shift by -17
- This is the same as shifting by +9, since 17+9 = 26

plaintext											
ciphertext	Y	v	c	c	f		n	f	i	c	u

UMASS CYBERSEC CLUB

Decrypt Caesar Cipher Example

- To undo Caesar Cipher, we shift again
- Go from the inner wheel to the outer wheel
- To undo a shift of +17, we shift by -17
- This is the same as shifting by +9, since 17+9 = 26

plaintext	H	e	l	l	o		w	o	r	l	d
ciphertext	Y	v	c	c	f		n	f	i	c	u

UMASS CYBERSEC CLUB

Caesar's Favorite Number, Parts 1 and 2

Challenge time!

Experiment with the Caesar Cipher!

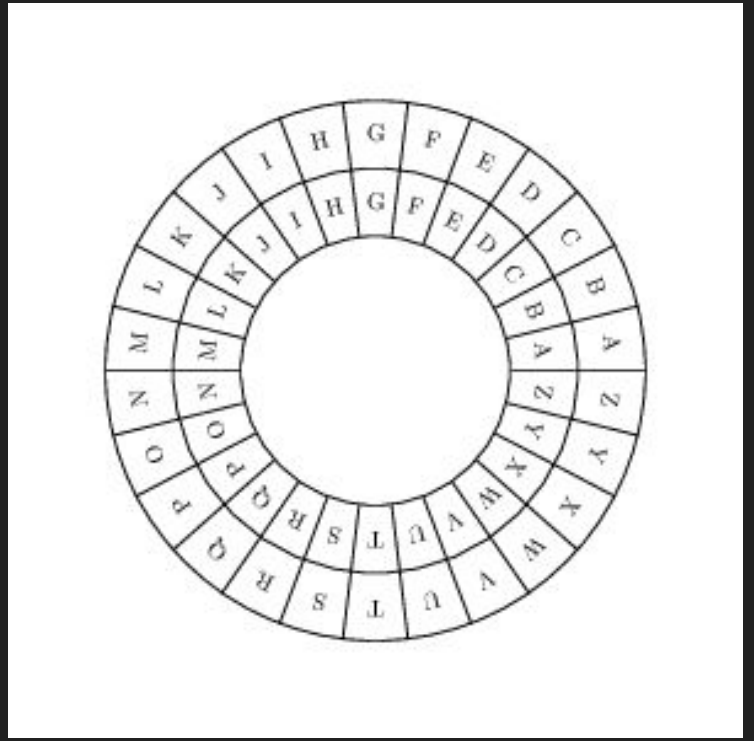
Try encoding and decoding the samples.

https://training.umasscybersec.org/

UMASS CYBERSEC CLUB

How Do We Break Caesar Cipher?

- Iterate over all possible keys
- There are only 26
- We can tell which is the correct one
- This a **brute-force attack**
- This type of attack will work for any Caesar Cipher



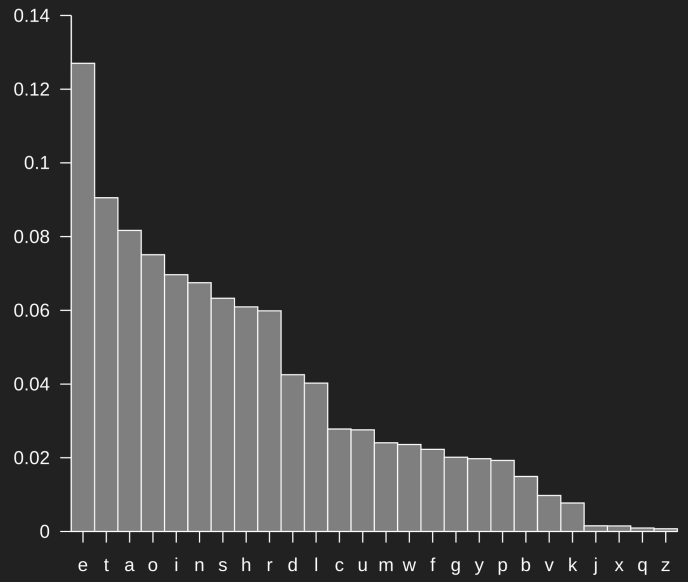
UMASS CYBERSEC CLUB

Break Caesar Cipher More!

- Is there any way of telling the computer which key should be right?
- What is your favorite Wordle starting word?

Break Caesar Cipher More!

- Is there any way of telling the computer which key should be right?
- What is your favorite Wordle starting word?
- One thing the Caesar Cipher does not hide is the **relative frequency** of different letters
- ‘E’ is the most common letter in the English alphabet
- If the shift is 3, ‘H’ will appear a lot in the ciphertext



UMASS CYBERSEC CLUB

Our Plan: Frequency Analysis

- Cycle through the 26 possible shifts
- Decrypt the ciphertext for each of those to get a candidate plaintext
- Assign each candidate a score, based on how often common letters occur
- Remember the best shift and the best score
- Return the best shift
- Use decrypt_caesar to reveal the plaintext!

```python
def break_caesar(message: bytes) -> int:
    """
    Attempts to break the Caesar cipher by trying
    """
    best_score = 0
    best_shift = 0
    for shift in range(26):
        decrypted = decrypt_caesar(message, shift)
        score = 0
        score += score_message(decrypted)
        if score > best_score:
            best_score = score
            best_shift = shift
    return best_shift
```

UMASS CYBERSEC CLUB

Caesar’s Favorite Number, Part 3

Challenge time!

Crack the Caesar Cipher and uncover Caesar’s letter!

https://training.umasscybersec.org/

UMASS CYBERSEC CLUB

How Can We Make Caesar Cipher Better?

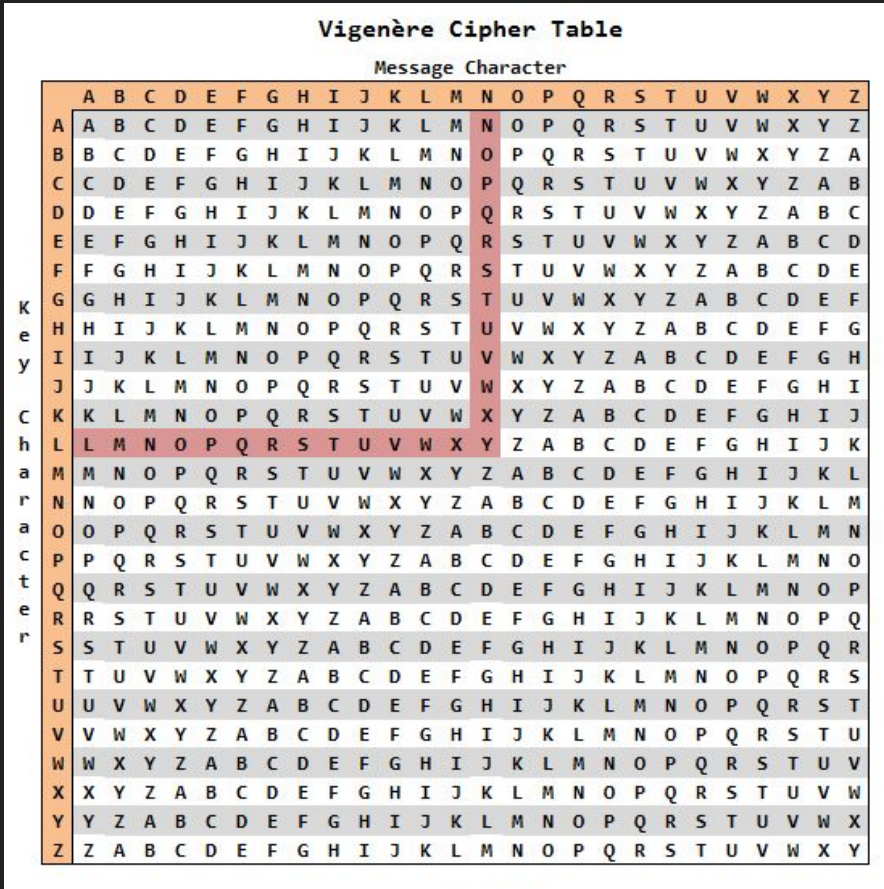
- The vulnerability came from too few keys, only 26
- Idea: make every shift correspond to a letter
- Caesar cipher uses one character to encrypt
- We can add more security by making a longer key
- Multiple shifts for different letters
- Enter, the Vigenère Cipher, a polyalphabetic cipher
- We repeat the key as many times as necessary
- This makes our cipher much harder to break

UMASS CYBERSEC CLUB

How to Vigenère

- Repeat the ciphertext as much as necessary
- Use the table to the right
- Ignore all non-alphabetic chars

plaintext	c	y	b	e	r	s	e	c
key	c	a	t	c	a	t	c	a
ciphertext								

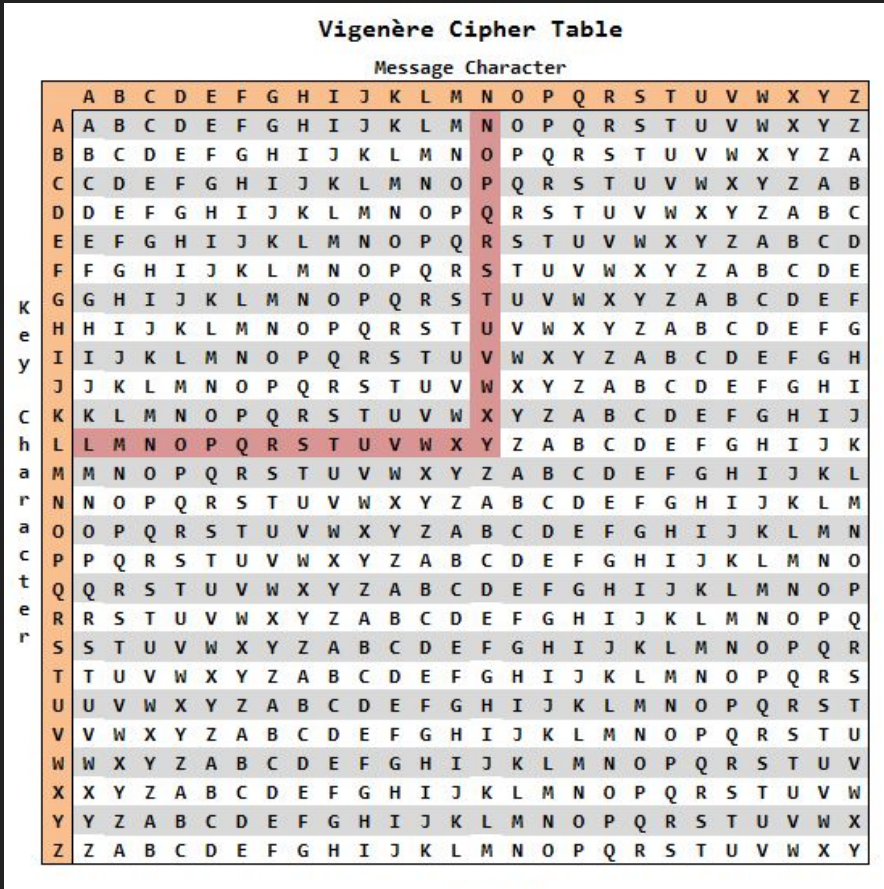


UMASS CYBERSEC CLUB

How to Vigenère

- Repeat the ciphertext as much as necessary
- Use the table to the right
- Ignore all non-alphabetic chars

plaintext	c	y	b	e	r	s	e	c
key	c	a	t	c	a	t	c	a
ciphertext	e	y	u	g	r	l	g	c



UMASS CYBERSEC CLUB

Take it for Granted, Parts 1 and 2

Challenge time!

Encrypt and decrypt the Vigenère Cipher!

https://training.umasscybersec.org/

UMASS CYBERSEC CLUB

How Do We Break Vigenère Cipher?

- We can reduce the problem to multiple Caesar ciphers
- Say we know the length of the key
- Then at regular intervals, it looks just like the Caesar cipher!
- Also, our same scoring technique works!
- We can build our key up from the individual chars of the Caesar cipher!

plaintext	c	y	b	e	r	s	e	c
key	c	a	t	c	a	t	c	a
ciphertext	e	y	u	g	r	l	g	c

Frequency Analysis for Vigenère

- This attack works best if we know the length of the key
- We break the ciphertext into segments
- Each segment is made of characters from the message that we **encrypted with the same shift**
- We ensure this by choosing characters of the ciphertext every key length apart (3 for the previous example)
- We can break each segment with break_caesar!

```python
def break_vigenere_with_key_len(message: bytes, key_len: int) -> bytes:
    message = [i for i in message if chr(i).isalpha()]
    key = bytearray()
    for i in range(key_len):
        segment = message[i::key_len]
        # TODO: find the best character for this segment and append it to key
    return bytes(key)
```

UMASS CYBERSEC CLUB

Take it for Granted, Part 3

Challenge time!

Break the Vigenère Cipher!

(remember, the key length is 15)

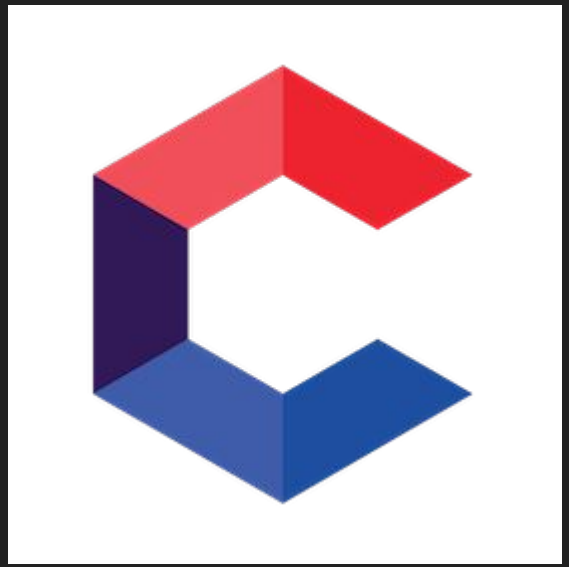
https://training.umasscybersec.org/

UMASS CYBERSEC CLUB

Now... some extra news!

UMASS CYBERSEC CLUB

Interested in Competing with us? Join CPTC2026!



UMASS CYBERSEC CLUB

Questions?

How do I learn more?
How can I get involved?
When are you guys available?

Come Up & Ask!

Resources Posted in Discord

Plus:
New Hacker Hours System!

Stay Tuned!

Newsletter

Discord ⭐

Twitter

Website

UMA
CYB