

# Cyber@UC Meeting 43

Cross-site scripting (XSS)  
CEH Cryptography and Recon

# If You're New!

- Join our Slack [ucyber.slack.com](https://ucyber.slack.com)
- **SIGN IN!**
- Feel free to get involved with one of our committees: **Content, Finance, Public Affairs, Outreach, Recruitment**
- **Ongoing Projects:**
  - Malware Sandboxing Lab
  - Cyber Range
  - RAPIDS Cyber Op Center



# Announcements

- We will be **running a CTF** at the **RevUC Hackathon!**
- **Sport Team Updates?**
- **Still Planning to visit DEFCON 2018**
- We are now an **official organization!**



## Eligibility:

Applicants must be citizens or permanent residents of the United States. Preference will be given to students whose home institutions have very limited or no research program in cyber security. Women and minorities are strongly encouraged to apply.



## Research Topics:

- Network Security
- Intrusion Detection
- Wireless Sensor Network Security
- Internet Malware Detection, Analysis, and Mitigation
- Software Reverse Engineering Vulnerability Discovery
- Privacy-Preserving Data Mining

## Support:

- \$5,000 stipend for 10 weeks
- Housing provided at no charge
- \$1,200 food allowance for 10 weeks
- Travel funds up to \$700 from/to the program



## Review:

The review of applications will begin **March 7, 2018** and will continue until all positions are filled.

For more information, please visit  
[reu.cs.wright.edu](http://reu.cs.wright.edu) or contact  
Dr. Junjie Zhang  
[junjie.zhang@wright.edu](mailto:junjie.zhang@wright.edu) 937-  
775-5015.

# Research Experience for Undergraduates Summer 2018

## Cyber Security Research May 14 – July 20



# ASME E-FEST

**An engineering festival  
is coming to Penn State  
this spring!**



**THREE DAYS**



**ENGINEERING  
COMPETITIONS**



**CAREER ADVICE  
& MENTORING**



**INTERACTIVE  
EXPERIENCES  
& NETWORKING**



**WORKSHOPS  
& SESSIONS**



**ENTERTAINMENT  
& FUN**

First 50  
students to  
register get  
a **FREE** ticket!  
Book using code  
**EFTEAST50**

**ASME E-Fests™**



Brought to you by ASME Engineering Festivals™.

# E-FEST EAST

**April 13th - 15th, 2018  
Penn State**



# Public Affairs

- Please fill out Google form for **GroupMe** Numbers!  
<https://goo.gl/forms/94i9kMJgtpDGXsC22>
- Our brand new **YouTube** channel has just been made. We will be live streaming meetings, events, etc and posting relevant videos to the channel. Please subscribe!  
[youtube.com/channel/UCWcJuk7A\\_1nDj4m-cHWvIFw](youtube.com/channel/UCWcJuk7A_1nDj4m-cHWvIFw)

## Follow us on our social media:

**Facebook:** <facebook.com/CyberAtUC/>

**Twitter:** <twitter.com/UCyb3r>

**Instagram:** <instagram.com/cyberatuc/>

**Website:** <gauss.ececs.uc.edu/UC.yber/>

# Weekly Content

# Unicode Character Crashes Apple Devices

- Using one of two unicode characters from a non-english language, Telugu, apple devices crash when displaying these characters if the default font San Francisco is being used
- Some of the vulnerable devices
  - Mail, Twitter, Messages, Slack, Instagram, WhatsApp, Gmail, and Facebook
- When the crash occurs, the app is irreparably damaged and must be uninstalled and reinstalled
- This is the second text crash found in apple devices already this year
  - A url was being used to crash phones back in january
- The bug has since been patched



# Apple crash sources

<https://techcrunch.com/2018/02/15/iphone-text-bomb-ios-mac-crash-apple/>

<https://support.apple.com/en-us/HT208535>

<https://techcrunch.com/2018/01/23/the-latest-ios-update-fixes-a-glitch-that-would-let-others-crash-your-phone-with-a-text-message/>

<https://www.theverge.com/2018/2/15/17015654/apple-iphone-crash-ios-11-bug-i-message>

<http://www.kcra.com/article/apple-text-bomb-can-crash-iphones-with-single-messages/18237239>


# Siemens Global Cybersecurity Initiative

- Siemens leads, IBM, Airbus, Allianz, Daimler, NXP, SGS, T-Mobile, and the Munich Security Conference in a new effort at making cybersecurity a major component and philosophy for businesses and governments
- This has been called the Charter of Trust
- It focuses on protecting data of individuals and businesses and preventing harm to critical infrastructure from cyber attacks
- The hope is for this charter to be made into global policy standards

<https://www.darkreading.com/threat-intelligence/siemens-leads-launch-of-global-cybersecurity-initiative/d/d-id/1331083>



# Swift Network used in bank heist

- \$2 million dollars were stolen from India's City Union Bank through the SWIFT financial network
  - This comes after an attack in Russia last Friday that stole \$6 million from the SWIFT network
  - SWIFT stands for Society for Worldwide Interbank Financial Telecommunications
  - A messaging network that banks use to securely transmit instructions and messages between each other
  - So far no sign of internal malicious behavior
- 

# SWIFT Network Sources

[https://www.darkreading.com/attacks-breaches/swift-network-used-in-\\$2-million-heist-at-indian-bank/d/d-id/1331092](https://www.darkreading.com/attacks-breaches/swift-network-used-in-$2-million-heist-at-indian-bank/d/d-id/1331092)

<https://www.darkreading.com/risk/central-banks-propose-better-inter-bank-security/d/d-id/1330006>

<https://www.investopedia.com/articles/personal-finance/050515/how-swift-system-works.asp>



# Part 3: Cryptography

You're here because you don't have  
Valentine's day plans





# The Topics Today Go Something Exactly Like This

- Cryptographic Methods
  - Shift Ciphers
  - Hashing
  - Single Key Encryption (Synchronous)
  - Public-Private Key Pairs (Asynchronous)
- Tool Overviews
  - HASHNAMEsum
  - John the Ripper (JTR)
- 127.0.0.1 on the range
  - Find & crack the real document



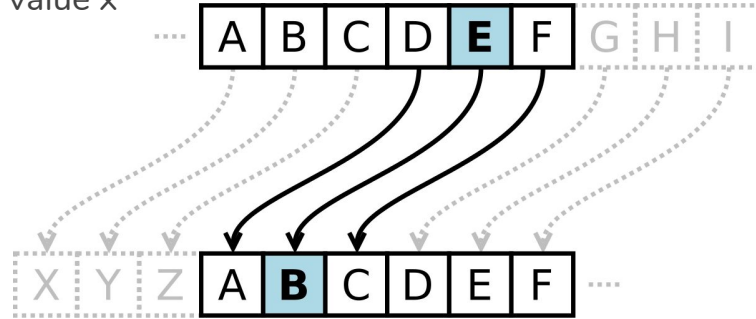
Put on your ~~3D glasses~~ **Linux Distro**  
now





# Cryptographic Method: ROTx Cipher

- Good in ancient times when only important people could read
- You change all the letters based on a chosen shift value  $x$
- Sometimes also called caesar cipher when  $x = 3$
- Biggest Weakness: widespread literacy



**'DEF'** becomes **'ABC'** in ROT3





# Cryptographic Method: Polyalphabetic Cipher

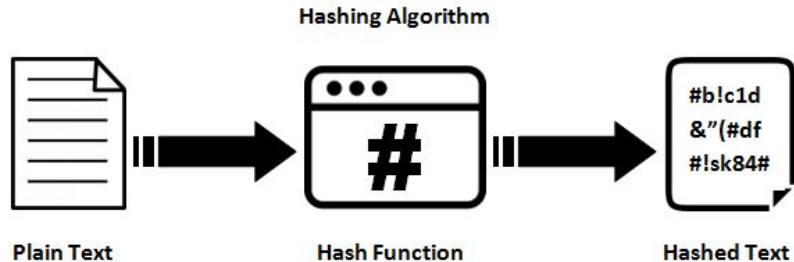
- Take the previous method and give it more than one shift value
- The new shift value set, or key breaks up our message
- Shorter keys are weak because we can use the use frequency of letters in any given alphabet to try to guess what the encrypted value is
- Longer keys are better because you use a short message and keep each key value unique to prevent decryption
- Weakness: both the encryptor and decryptor must have the same key

**'DEF'** becomes **'ABC'** with key **555**

**'DEF'** becomes **'AAA'** with key **567**

# Cryptographic Method: Hashing

- Hashes are **one way** cryptographic functions, the output is not meant to be decoded
- Used to verify data integrity in things such as radio signals
- Also used to store passwords in databases so that they aren't in plaintext but can still be used for authentication
- Ideally  $f(\text{in}) = \text{out}$  such that  $g(\text{out}) = \text{in}$  so that no two inputs have the same hash
  - However because hash functions have set size outputs, there will be 'collisions'
- Weakness: hash functions with small length outputs will have multiple **in's** for any **out**
- Popular hashes include Secure Hashing Algorithm (SHA) and Cyclic Redundancy Check (CRC)



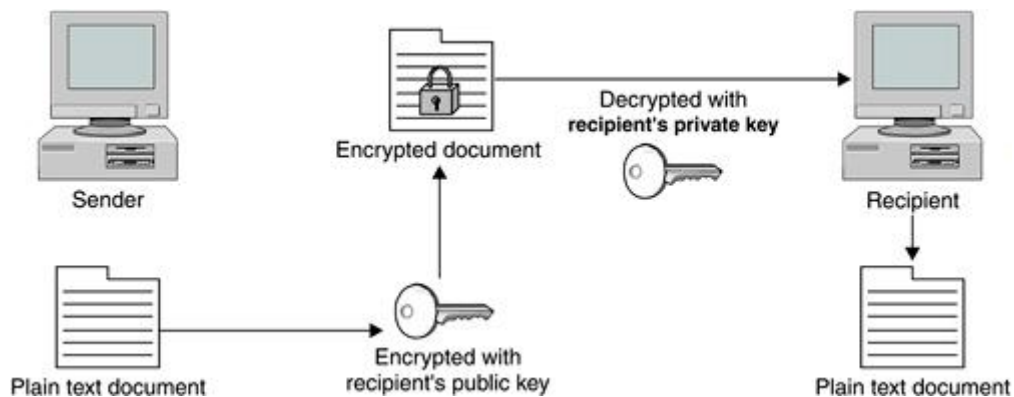


## Cryptographic Method: Synchronous Keys

- The new shift value set, or key breaks up our message
- Instead of shifting letters predictably, very mathematical math is used
- Longer keys are better because you use a short message and keep each key value unique to prevent decryption
- Weakness: both the encryptor and decryptor must have the same key
- Unlike hashes the function is two way and is meant to be reversed but only when the same encryption key is used to encrypt and decrypt
- Used to ensure data Confidentiality

# Cryptographic Method: Key Pairs

- With key pairs two keys are used
- **Public key - encrypts data**
- **Private key - decrypts data**
- This method is very slow but can be used to share a large key for synchronous crypto methods in a secure way. This is how SSL works.





# Tool Overview: HASHNAMEsum

- Installed already on most Linux systems, especially Kali

Hash Function	Hash Length (bigger = better)	Command
MD5	128	md5sum
SHA-1	160	sha1sum
SHA-224	224	sha224sum
SHA-256	256	sha256sum
SHA-384	384	sha384sum
SHA-512	512	sha512sum

# Tool Overview: John the Ripper (JTR)

- Installed already on Kali, otherwise: `cd /opt; git clone https://github.com/magnumripper/JohnTheRipper`
- Fast password cracking tool
- Auto-detects hash types
- Can use both dictionary (known password) attacks and brute force attacks
- Can extract password hashes from various local files
- Can crack password hashes stored in databases





# Tool Overview: Word Lists

- Words Lists are gathered from real world resources such as studies and actual password leaks
- Word Lists contain commonly used passwords from various sources
- <https://github.com/danielmiessler/SecLists> has a well maintained set of passwords lists as well as other security related lists such as common usernames
- JTR and Hashcat can hash the passwords on the list and compare them to the target hashes very quickly to try and quickly identify the plaintext of the hash
- Kali has some preloaded lists



# Hashing and Cracking!

- To hash a file: `md5sum <file>`

Lets try hashing a “password” with md5 sum!

- `echo -n “Password1” | md5sum | tr -d “ -” >> hashes`

And let’s crack it:

- `john --format=raw-md5 ~/hashes --show`
- `john --format=raw-md5 ~/hashes --wordlist=/opt/SecLists/Passwords/rockyou.txt`





# 127.0.0.1 on the Range

- It's **way past** Valentine's day and I **still** can't login to the CYBER@UC email account to see all our love letters.
- I did happen to accidentally download all of my emails as password protected PDF's that I don't have the passwords to.
- Your challenge is to:
  - Find the email with a **MD5 hash that contains d46922f57d032d987c**
  - Find the password to that PDF using **JTR** against the possible hashes file
  - **Don't open that email just yet!** Come up to the front to show everyone how you did it then open the email for all of us to see.

# 127.0.0.1 on the Range (extra)

- Crack all the PDF's!

