Ethical Student Hackers

Cryptography

The Legal Bit

- The skills taught in these sessions allow identification and exploitation of security vulnerabilities in systems. We strive to give you a place to practice legally, and can point you to other places to practice. These skills should not be used on systems where you do not have explicit permission from the owner of the system. It is VERY easy to end up in breach of relevant laws, and we can accept no responsibility for anything you do with the skills learnt here.

- If we have reason to believe that you are utilising these skills against systems where you are not authorised you will be banned from our events, and if necessary the relevant authorities will be alerted.

- Remember, if you have any doubts as to if something is legal or authorised, just don't do it until you are able to confirm you are allowed to.

Code of Conduct

- Before proceeding past this point you must read and agree to our Code of Conduct - this is a requirement from the University for us to operate as a society.
- If you have any doubts or need anything clarified, please ask a member of the committee.
- Breaching the Code of Conduct = immediate ejection and further consequences.
- Code of Conduct can be found at https://shefesh.com/downloads/SESH%20Code%20of%20Conduct.pdf

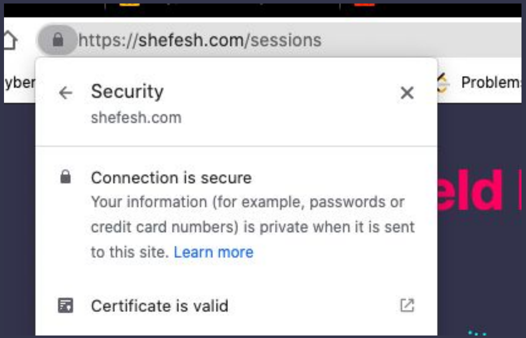
Introduction of Cryptography

Cryptography is the science of how to protect your own information and messaging and how to decipher enemy information .

Based on the emergence of the public key cryptography system represented by RSA, the development of cryptography can be divided into classical cryptography and modern cryptography.

Cryptography is everywhere in life.

https, SSL/TLS



https://shefesh.com/sessions

Security
shefesh.com

Connection is secure
Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Certificate is valid

Decryption algorithms

Digital signatures

Message Authentication - Hash

The History of Cryptography

Before 1949, Cryptography was not yet a science, but an art.

Some cryptographic algorithms and encryption devices emerge.

Cryptographers of this period often approached cryptography and analysis by intuition and belief, rather than by reasoned proof.

Simple cryptanalysis techniques emerge.

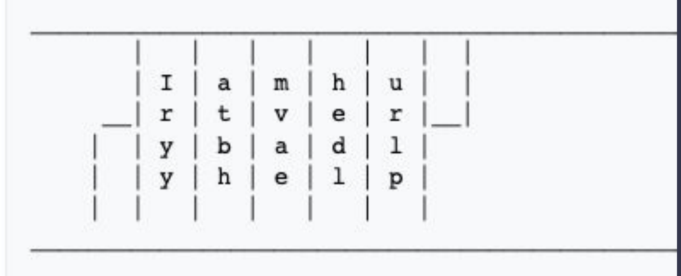
The basic means of cryptographic algorithms (substitution & permutation) emerge, targeting characters

Scytale Cipher

In cryptography, a scytale is a tool used to perform a transposition cipher, consisting of a cylinder with a strip of parchment wound around it on which is written a message. The ancient Greeks, and the Spartans in particular, are said to have used this cipher to communicate during military campaigns.

The recipient uses a rod of the same diameter on which the parchment is wrapped to read the message.

“I am hurt very badly help” -> "Iryyatbhmvaehedlurlp"



```
| I | a | m | h | u |
| r | t | v | e | r |
| y | b | a | d | l |
| y | h | e | l | p |
```

https://en.wikipedia.org/wiki/Scytale#

Caesar Cipher

Caesar cipher, the shift cipher, one of the simplest and most widely known encryption techniquies.

Left shift of 3

Plain	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
Cipher	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

“DOG” -> “ALD”

“APPLE” -> ”XMMIB”

https://drive.google.com/file/d/1VolG0GqULfNuGFRg3MsCfKpz4AMBk4WQ/view?usp=sharing

Enigma Cipher

The Enigma machine was invented by German engineer at the end of World War I.
Pre-war German military planning emphasized fast, mobile forces and tactics, later known as blitzkrieg, which depend on radio communication for command and coordination. Since adversaries would likely intercept radio signals, messages had to be protected with secure encipherment. Compact and easily portable, the Enigma machine filled that need.

During World War II, mathematicians and engineers used mathematical knowledge and science to decipher the German "Enigma" and "Lorentz" codes,
as well as the Japanese naval codes,
to obtain a large amount of “super intelligence ”
which led to the reversal of the war.

https://en.wikipedia.org/wiki/Typex

Practice

Register an account on the CRYPTOHACK website

https://cryptohack.org/register/

Arts -> Science

More and more mathematicians join the cryptography team.

In 1949, the release of “The Communication Theory of Secret Systems, Shannon” . Arts -> Science

Symmetric-key Cryptography. DES

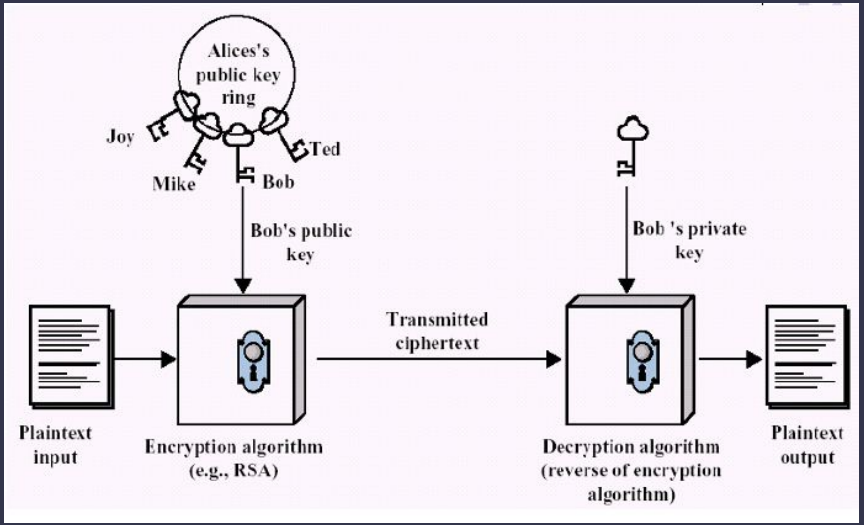
Public-key Cryptography. RSA

Digest Function. Hash

RSA

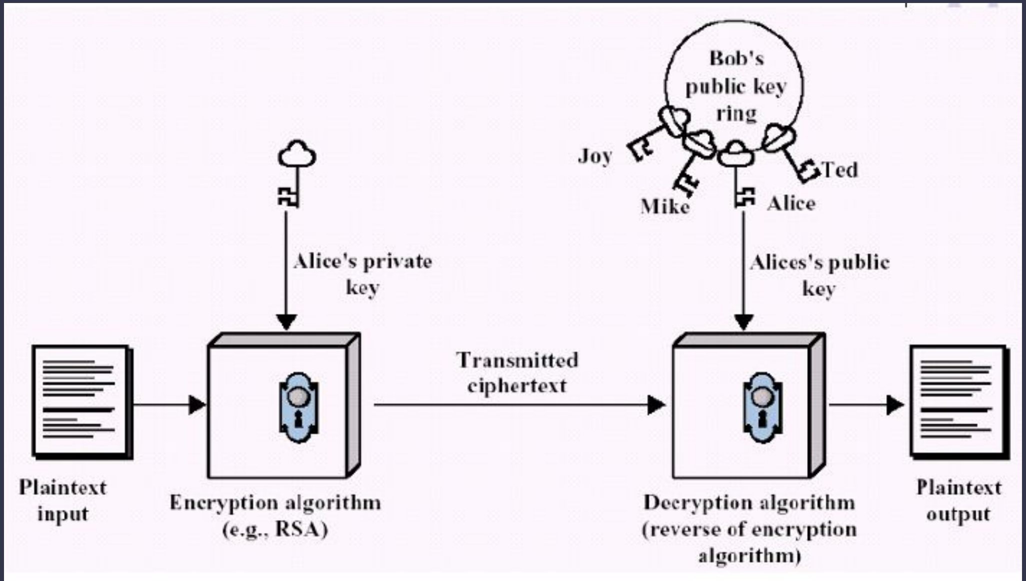
First described in 1977, RSA is the most famous public-key cryptosystem.

Public enables a user, Bob, to distribute a public key and others can use that public key to encrypt messages to her. Bob can then use her private key to decrypt the messages.



RSA

- Digital signatures enable Alice to use her private key to "sign" a message. Anyone can use Alice's public key to verify that the signature was created with her corresponding private key, and that the message hasn't been tampered with.



RSA - Algorithms

N = p*q which ‘p’ and ‘q’ are two primes

Euler totient of N: φ(N) = (p-1)*(q-1)

exponent ‘e’ and φ(N) are prime to each other

d * e = 1 mod φ(N). □ d * e = φ(n) * K + 1 (Modular multiplicative inverse)

Public key: {e, N}
Private key: {d, N}

Ciphertext = Plaintext^e mod N
Plaintext = Ciphertext^e mod N

Hash

- A hash function is a function which takes an arbitrary long string of bits and produces a fixed-length output.
- Cryptographic hash function are designed to be one-way: functions that are practically impossible to invert.
- Cryptographic hash functions are used to verify message integrity, compute digital signatures, and safely store passwords in databases.

SQL Injection & Hash

http://18.130.232.203/DVWA/login.php

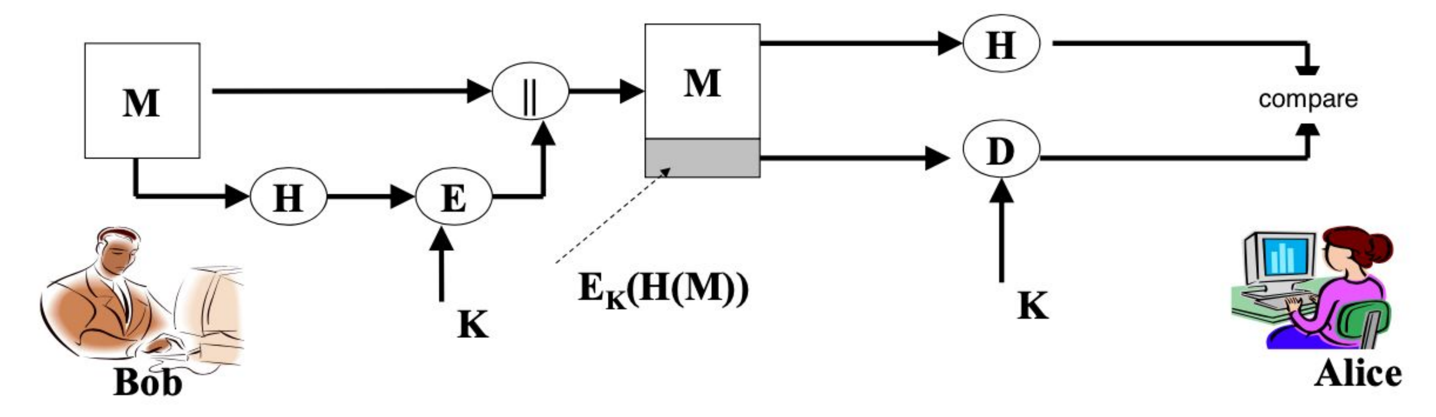
sesh
sqlinjection_hash

```
1' or 1=1 union select user, password from users#
```

https://www.dcode.fr/hash-function

Hash

- Message authentication
- Digital signatures



Hashcat - Manual Hash Cracking

You can also use hashcat, a powerful tool installed on Kali, to crack many hash formats

Basic Command:

```
hashcat -a 0 -m [MODE] –wordlist /usr/share/wordlists/rockyou.txt [HASH_FILE]
```

Common Formats:

- MD5: 0
- PHPass (Wordpress): 400
- Find a hash format: `hashid [HASH] | awk '{print $2}' | while read line; do hashcat --example-hashes | grep $line -B 1; done`

If hashcat tells you that your file format is invalid, try using `echo -n HASH > hashfile` or stripping the last character of the file

Generate a wordlist: `hashcat --force --stdout [PASSWORDS] -r /usr/share/hashcat/rules/best64.rule > passwordlist`

Practice

RSA

https://cryptohack.org/challenges/rsa/

HASH

https://cryptohack.org/challenges/hashes/

Upcoming Sessions

What’s up next?

www.shefesh.com/sessions

(14/03/22): Cryptography

(21/03/22): Advanced Web Hacking

(28/03/22): CTF and possible session?

(04/04/2022): HTB Session

(25/Apr/2022): HTB Session

Any Questions?

www.shefesh.com

Thanks for coming!