Crypto CTF Challenge

Mustakimur Rahman Khandaker

Introduction

http://ctf.cs.uga.edu:8000/

Cryptography is the reason we can use banking apps, transmit sensitive information over the web, and in general protect our privacy.

A large part of CTFs is breaking widely used encryption schemes which are improperly implemented.

- The math may seem daunting, but more often than not, a simple understanding of the underlying principles will allow you to find flaws and crack the code.

Cryptic	Factored	Conflict	Vigenere 5	What's that?
You get a screenshot of an encrypted file. Find the flag.	You intercept RSA encrypted messages between bob and alice. Find the flag.	We develop a hash for password to protect sensitive data.	You have received intercepted a cryptic message. Find the flag.	You have seen a morse code. But, do you know what it stands for?
Pts: 15	*Pts: 75*	*Pts: 50*	*Pts: 30*	*Pts: 75*

XOR

An XOR or *eXclusive OR* is a bitwise operation indicated by `^` and shown by the following truth table:

A	B	A ^ B
0	0	0
0	1	1
1	0	1
1	1	0

```
>>> data = 'CAPTURETHEFLAG'
>>> key = 'A'
>>> encrypted = ''.join([chr(ord(x) ^ ord(key)) for x in data])
>>> encrypted
'\x02\x00\x11\x15\x14\x13\x04\x15\t\x04\x07\r\x00\x06'
>>> decrypted = ''.join([chr(ord(x) ^ ord(key)) for x in encrypted])
>>> decrypted
'CAPTURETHEFLAG'
```

Single Byte XOR Encryption

Single Byte XOR Encryption is trivial to bruteforce as there are only 255 key combinations to try.

Caesar Cipher/ROT 13

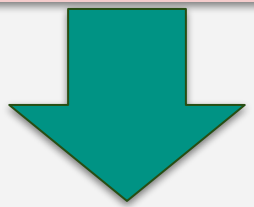
The Caesar Cipher or Caesar Shift is a cipher which uses the alphabet in order to encode texts.

CAESAR encoded with a shift of 8 is KIMAIZ so ABCDEFGHIJKLMNOPQRSTUVWXYZ becomes IJKLMNOPQRSTUVWXYZABCDEFGH

ROT13 is the same thing but a fixed shift of 13.

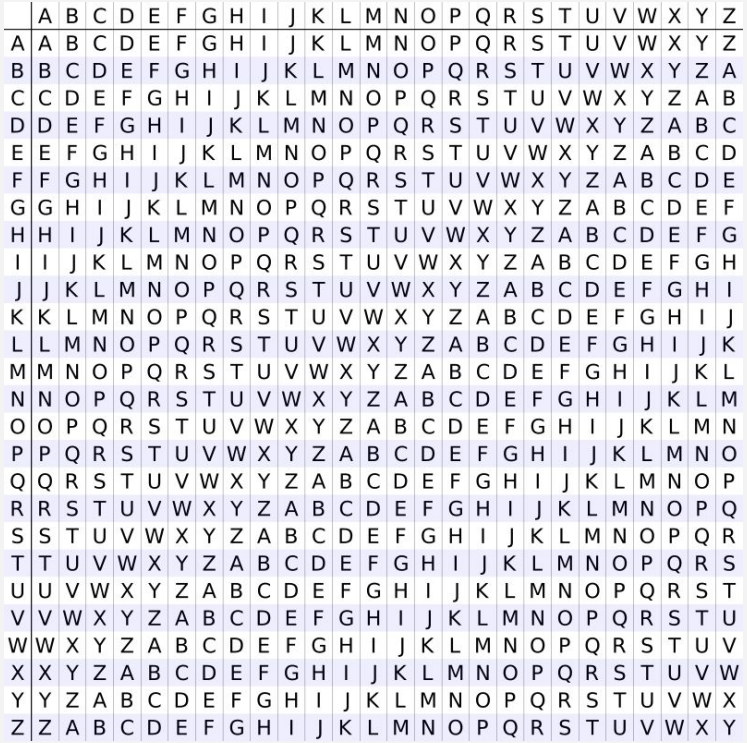
- Because there are 26 letters (2×13) in the basic Latin alphabet, ROT13 is its own inverse.

Google_2016_OCR_is_Cool:
Caesar once said, don't stab me… but taking a screenshot of an image sure feels like being stabbed. You connected to a VNC server on the Foobanizer 9000, it was view only. This screenshot is all that was present but it's gibberish. Can you recover the original text?



Vigenere Cipher

A Vigenere Cipher is an extended Caesar Cipher where a message is encrypted using various Caesar shifted alphabets.



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

Encryption

For example, encrypting the text SUPERSECRET with CODE would follow this process:

- CODE gets padded to the length of SUPERSECRET so the key becomes CODECODECOD
- For each letter in SUPERSECRET we use the table to get the Alphabet to use, in this instance ***row C and column S***
- The ciphertext's first letter then becomes U
    - We eventually get UISITGHGTSW

Hashing Functions

Hashing functions are one way functions which theoretically provide a unique output for every input.

- MD5, SHA-1, and other hashes which were considered secure are now found to have collisions.

A string hash is a number or string generated using an algorithm that runs on text or data.

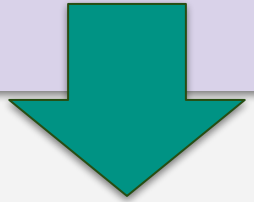
```
$ echo -n password | md5sum
5f4dcc3b5aa765d61d8327deb882cf99
```

A file hash is a number or string generated using an algorithm that is run on text or data.

```
$ md5sum samplefile.txt
3b85ec9ab2984b91070128be6aae25eb samplefile.txt
```

There was this student hash design contest. All submissions were crap, but had promised to use the winning algorithm for our important school safe. We hashed our password and got "00006800007d". Brute force isn't effective anymore and the hash algorithm had to be collision-resistant, so we're good to go, aren't we?

File: crypto70.zip



RSA

https://github.com/Ganapati/RsaCtfTool

RSA is a cryptosystem which allows for asymmetric encryption.

- Asymmetric cryptosystems are commonly referred as **Public Key Cryptography.**
  - where a *public key* is used to encrypt data and only a secret, *private key* can be used to decrypt the data.

The Public Key is made up of ***(n, e)***

The Private Key is made up of ***(n, d)***

p and ***q*** are prime numbers which make up ***n***

n is the modulus and its length in bits is the bit length

e is the public exponent

d is the private exponent

Key Generation

- Choose two prime numbers such as:
  p = 61 and q = 53
- Find n:
  n = pq = 3233
- And so on, ….

Alice wants to send Bob a confidential message. They both remember the crypto lecture about RSA. So Bob uses openssl to create key pairs. Finally, Alice encrypts the message with Bob's public keys and sends it to Bob. Clever Eve was able to intercept it. Can you help Eve to decrypt the message?

Extra

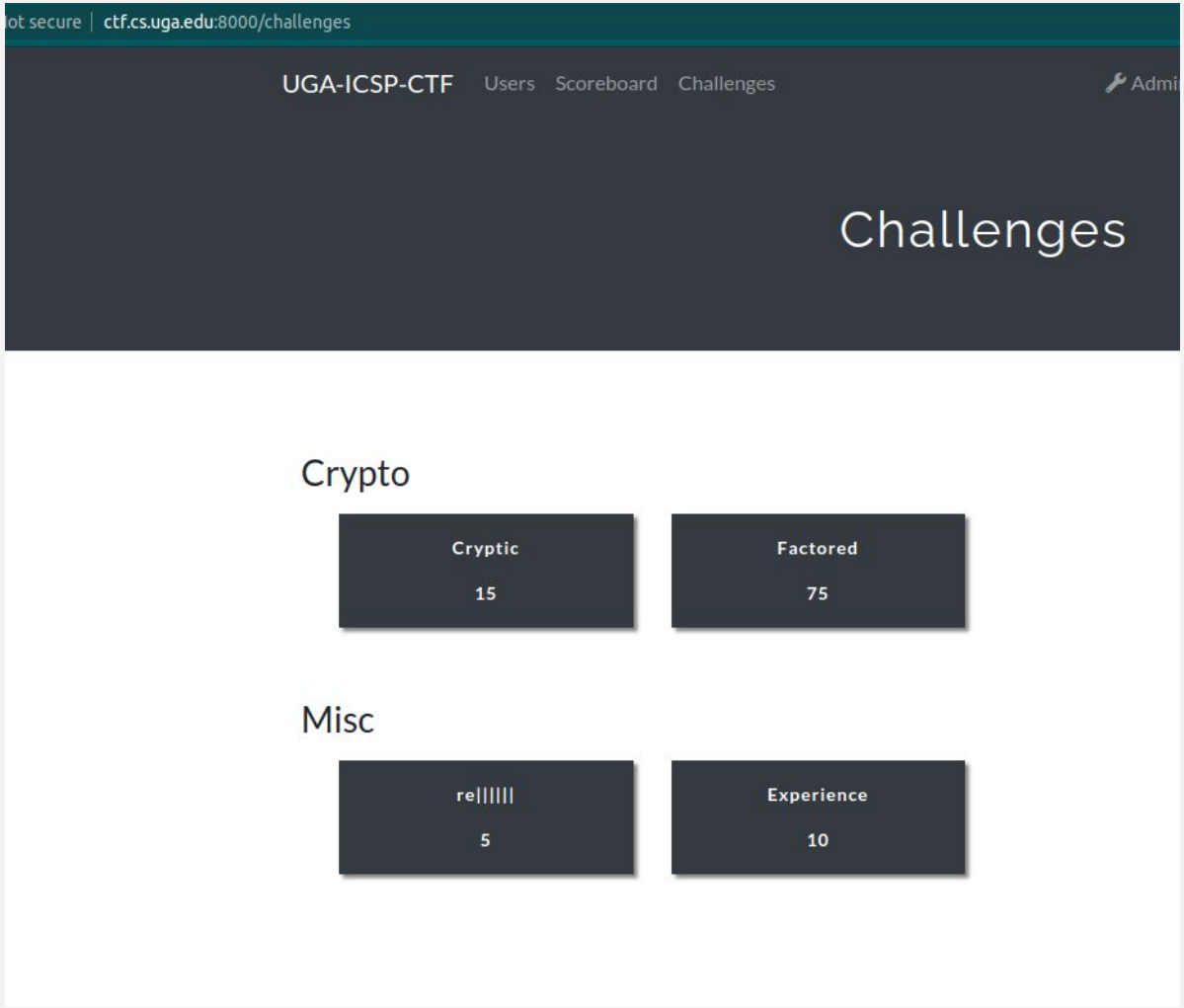
https://archive.ooo/c/goo-or-ooo/408/

https://archive.ooo/c/ooo-flag-sharing/366/

https://archive.ooo/c/nooombers/405/

https://github.com/internetwache/Internetwache-CTF-2016/tree/master/tasks/crypto80

https://github.com/internetwache/Internetwache-CTF-2016/tree/master/tasks/crypto90


ot secure | ctf.cs.uga.edu:8000/challenges
UGA-ICSP-CTF
Users
Scoreboard
Challenges
Admi
Challenges
Crypto
Cryptic
15
Factored
75
Misc
rel||||||
5
Experience
10

Next:
Web Exploit