CTF-0

KNOWLEDGE SESSION

Cybersecurity??

Cybersecurity

Cybersecurity

Red team

Blue team

What's a CTF?

putting the Hack in Hackathon

What's a CTF?

ctfZero{b4s3d_4nd_r3dp1ll3d_7d5be18a}

There is a hidden string, called a 'flag'
which we have to find out!

Techniques

Forensics

Forensics is the art of recovering the digital trail left on a computer. Using this, we can access data that is supposedly "lost".

Website for basic file forensics

To Alan Rodriguez, with Love

Techniques

Cryptography

Cryptography is the technique of securing information and communication using certain codes.

Primitive examples: Caesar, Atbash ciphers

Present-day examples: RSA, AES

Techniques

Web Exploitation

Using bugs and vulnerabilities present in websites to access hidden data or hijack a server

Common techniques: SQL injection, XSS, CSRF

Link to a very good resource

Techniques

Reverse Engineering

```c
#include <stdio.h>

int main() {
    printf("Hello, world!\n");
    return 0;
}
```

compilation (easy) →

← decompilation (hard)

```asm
push rbp
mov rbp, rsp
lea rax, str.Hello__world_
mov rdi, rax
call sym.imp.puts
mov eax, 0
pop rbp
ret
```

source code:
humans like
computers hate

machine code:
humans hate
computers like

ROM hacks

Techniques

Binary Exploitation

Binaries are files that computers can execute. We find bugs in binaries that let us make them perform unintended behavior.

Amazing playlist

Quick Question:

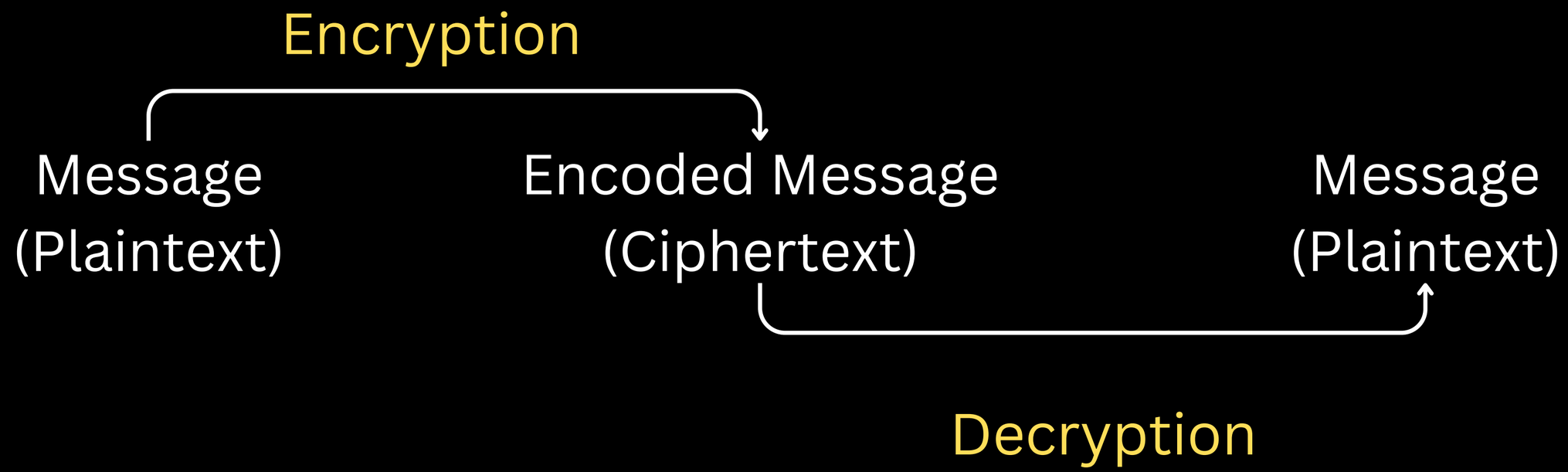
Reverse Engineering

We talked about our code being compiled into assembly language, and finally to machine code.

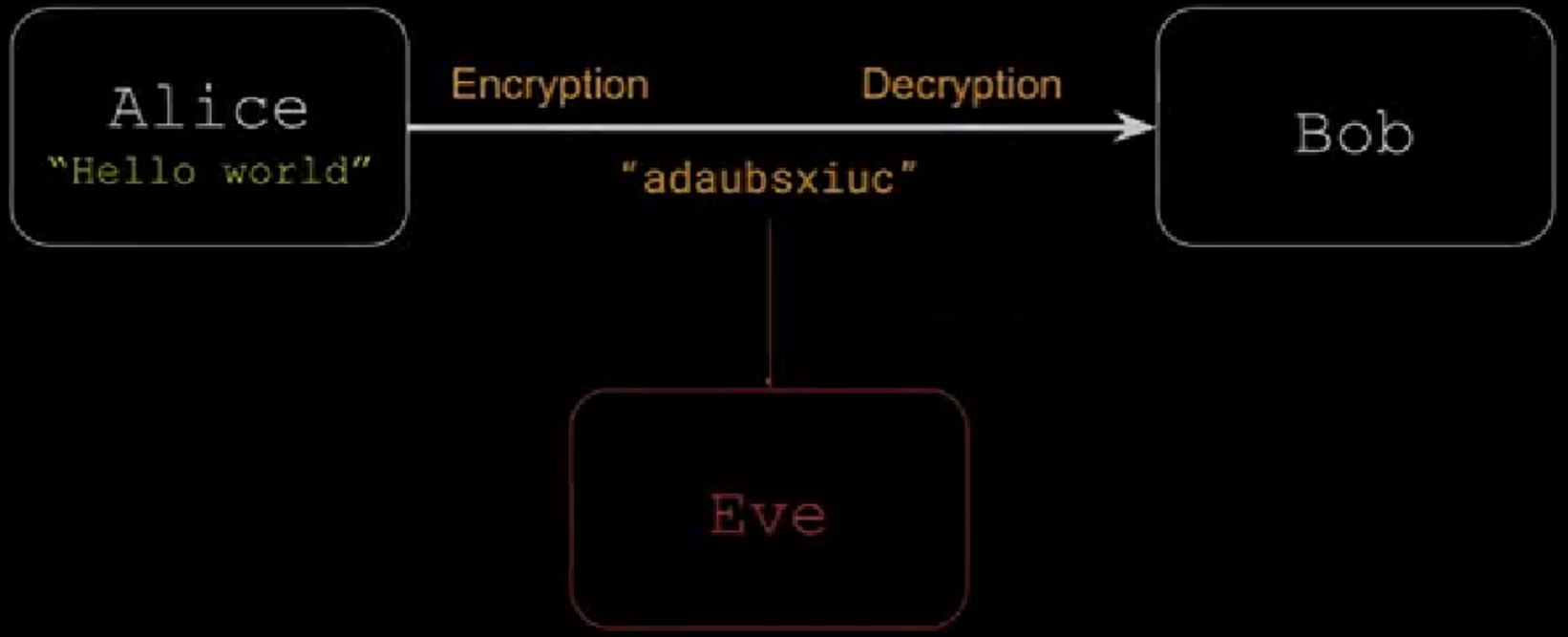
Can you name programming languages which compile our code?
Are there any programming languages which don't do this?

Cryptography

Cryptography is the technique of securing information and communication using certain codes.



Cryptography



Caesar (ROT) Cipher

Example 1:

a -> b
b -> c
c -> d
and so on
z -> a

Shift = +1

Example 2:

a -> d
b -> e
c -> f
and so on

w -> z
x -> a
y -> b
z -> c

Shift = +3

Caesar Cipher

How to "break" the Caesar Cipher?

Simple Brute Force attack can do it!

Caesar Cipher

Idea: Iterate over all possible shifts, and select the correct one!

For example, consider the ciphertext "gdkkn"

Possibilities:

- Shift=1: "hello"
- Shift=2: "ifmmp"

and so on!

Among these, only Shift=1 produces a sensible English word

Caesar Cipher

```
For key 0, decrypted text: ks gvozz ohhoqy hvsa tfca hvs tfcbh oh bccb cb Tisgrom
For key 1, decrypted text: jr funyy nggnpx gurz sebz gur sebag ng abba ba Thrfqnl
For key 2, decrypted text: iq etmxx mffmow ftqy rday ftq rdazf mf zaaz az Tgqepmk
For key 3, decrypted text: hp dslww leelnv espx qczx esp qczye le yzzy zy Tfpdolj
For key 4, decrypted text: go crkvv kddkmu drow pbyw dro pbyxd kd xyyx yx Teocnki
For key 5, decrypted text: fn bqjuu jccjlt cqnv oaxv cqn oaxwc jc wxxw xw Tdnbmjh
For key 6, decrypted text: em apitt ibbiks bpmu nzwu bpm nzwvb ib vwwv wv Tcmalig
For key 7, decrypted text: dl zohss haahjr aolt myvt aol myvua ha uvvu vu Tblzkhf
For key 8, decrypted text: ck yngrr gzzgiq znks lxus znk lxutz gz tuut ut Takyjge
For key 9, decrypted text: bj xmfqq fyyfhp ymjr kwtr ymj kwtsy fy stts ts Tzjxifd
For key 10, decrypted text: ai wlepp exxego xliq jvsq xli jvsrx ex rssr sr Tyiwhec
For key 11, decrypted text: zh vkdoo dwwdfn wkhp iurp wkh iurqw dw qrrq rq Txhvgdb
For key 12, decrypted text: yg ujcnn cvvcem vjgo htqo vjg htqpv cv pqqp qp Twgufca
For key 13, decrypted text: xf tibmm buubdl uifn gspn uif gspou bu oppo po Tvftebz
For key 14, decrypted text: we shall attack them from the front at noon on Tuesday
For key 15, decrypted text: vd rgzkk zsszbj sgdl eqnl sgd eqnms zs mnnm nm Ttdrczx
For key 16, decrypted text: uc qfyjj yrryai rfck dpmk rfc dpmlr yr lmml ml Tscqbyw
For key 17, decrypted text: tb pexii xqqxzh qebj colj qeb colkq xq kllk lk Trbpaxv
For key 18, decrypted text: sa odwhh wppwyg pdai bnki pda bnkjp wp jkkj kj Tqaozwu
For key 19, decrypted text: rz ncvgg voovxf oczh amjh ocz amjio vo ijji ji Tpznyvt
For key 20, decrypted text: qy mbuff unnuwe nbyg zlig nby zlihn un hiih ih Toymxus
For key 21, decrypted text: px latee tmmtvd maxf ykhf max ykhgm tm ghhg hg Tnxlwtr
For key 22, decrypted text: ow kzsdd sllsuc lzwe xjge lzw xjgfl sl fggf gf Tmwkvsq
For key 23, decrypted text: nv jyrcc rkkrtb kyvd wifd kyv wifek rk effe fe Tlvjurp
For key 24, decrypted text: mu ixqbb qjjqsa jxuc vhec jxu vhedj qj deed ed Tkuitqo
For key 25, decrypted text: lt hwpaa piiprz iwtb ugdb iwt ugdci pi cddc dc Tjthspn
```

[Website for Brute-force]

Quick Question

Instead of Caesar Cipher, consider a cipher in which every letter of the alphabet gets mapped to some other letter. Of course, this mapping has to be invertible, because only then you can decrypt the text.

How many such encryptions are there?

ASCII code

Characters of English alphabet (both uppercase and lowercase), numbers, symbols (?, !, etc.), spaces are given unique standardized numbers

For example,

- ascii('a') = 97
- ascii('b') = 98
- ascii('A') = 65
- ascii('?') = 63

ASCII table

0	NUL	16	DLE	32		48	0	64	@	80	P	96	`	112	p
1	SOH	17	DC1	33	!	49	1	65	A	81	Q	97	a	113	q
2	STX	18	DC2	34	"	50	2	66	B	82	R	98	b	114	r
3	ETX	19	DC3	35	#	51	3	67	C	83	S	99	c	115	s
4	EOT	20	DC4	36	$	52	4	68	D	84	T	100	d	116	t
5	ENQ	21	NAK	37	%	53	5	69	E	85	U	101	e	117	u
6	ACK	22	SYN	38	&	54	6	70	F	86	V	102	f	118	v
7	BEL	23	ETB	39	'	55	7	71	G	87	W	103	g	119	w
8	BS	24	CAN	40	(	56	8	72	H	88	X	104	h	120	x
9	HT	25	EM	41	)	57	9	73	I	89	Y	105	i	121	y
10	LF	26	SUB	42	*	58	:	74	J	90	Z	106	j	122	z
11	VT	27	ESC	43	+	59	;	75	K	91	[	107	k	123	{
12	FF	28	FS	44	,	60	<	76	L	92	\	108	l	124	|
13	CR	29	GS	45	-	61	=	77	M	93	]	109	m	125	}
14	SO	30	RS	46	.	62	>	78	N	94	^	110	n	126	~
15	SI	31	US	47	/	63	?	79	O	95	_	111	o	127	DEL

How are strings stored in computer memory?

string = "CTF-0"

string	C	T	F	-	0
ASCII	67	84	70	45	48
Binary	01000011	01010100	01000110	00101101	00110000

XOR Operation

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

Bitwise XOR Operation

Convert number to binary, then take XOR of individual bits ("^" symbol in programming languages)

Example: What is 7 ^ 9?

7 is binary is 0111

9 in binary is 1001

Now, their bitwise XOR is 1110 = 14

Quick Question

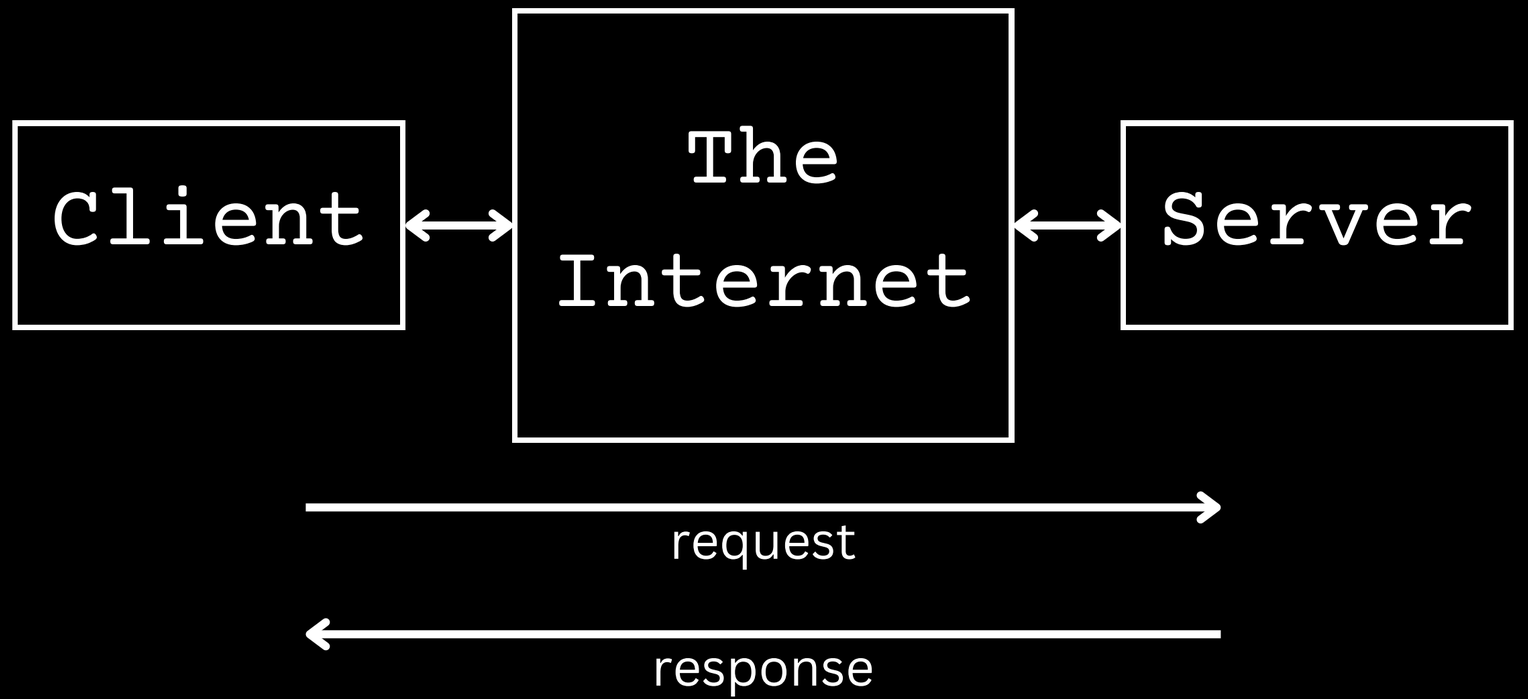
Alice has a hidden number m. To encrypt it, Alice takes the bitwise XOR of n with a key, called k, to obtain the encrypted message c.

c = m XOR k

c is publicly known, and c = 1011 (in binary). By some scam, the number k is known. k = 0110 (in binary).

Can you find the original number m?

Websites



Looks simple, but there is a lot of machinery in the background!

We use **protocols** to co-ordinate the internet.

Layers of the OSI Model

(open systems interconnection)

Application	"what does this data mean"
Presentation	"how do i encode this data before sending it out"
Session	"how do i know who's sending this data and in what context"
Transport	"how do i send this data to the right network"
Network	"how do i transmit data between different wires that people are using"
Data link	"how do i coordinate with others who wanna put data on the same wire"
Physical	"how do i put data on this wire"

Websites

The frontend

HTML (document structure)

CSS (design and colors)

JavaScript (functionality)

The backend

PHP/JavaScript/Python/... (server logic)

SQL (database management)

Linux/Windows/BSD (server backbone)

Let's look at a webpage!

Forensics

File formats have their own specifications.
They tell you how data is logically arranged in a file stored on the disk.

One common thing across formats is the file header.

You can use tools like frhed to view the bytes in files as they are, raw.

Forensics

If we look at the hex dump (i.e. hexadecimal representation of the bytes), the first few bytes are "magic bytes" used to denote the type of the file.

jpeg first few bytes are:

FF D8 FF E0 00 10 4A 46 49 46 00 01

Let's have a practical look!

Let's solve a crypto question!

Link to problem

How to view the HTML source?

Open your browser, right click on the desired webpage, select "view page source"

HTML of Google Homepage:

```
<!doctype html>
<html dir="ltr" lang="en">
  <head>
    <meta charset="utf-8">
    <title>New Tab</title>
    <style>
      body {
        background: #333333;
        margin: 0;
      }

      #backgroundImage {
        border: none;
        height: 100%;
        pointer-events: none;
        position: fixed;
        top: 0;
        visibility: hidden;
        width: 100%;
      }

      [show-background-image] #backgroundImage {
        visibility: visible;
      }
    </style>
  </head>
  <body>
    <iframe id="backgroundImage" src=""></iframe>
    <ntp-app></ntp-app>
    <script type="module" src="new_tab_page.js"></script>
    <link rel="stylesheet" href="chrome://resources/css/text_defaults_md.css">
    <link rel="stylesheet" href="chrome://theme/colors.css?sets=ui,chrome">
    <link rel="stylesheet" href="shared_vars.css">
  </body>
</html>
```

HTML

Programming language used to display webpages in web browsers

```
<!DOCTYPE html>
<html>
<body>
<h1>My First Heading</h1>
<p>My first paragraph.</p>
</body>
</html>
```