Cryptography

SLIDES BY MIGUEL

22/11/2023

CTF CAFE

What is Crypto?

Encoding vs Encryption

Maths!

Key Exchange, Symmetric, Asymmetric

Ciphers

Data Representation

Hashing

Encoding is NOT Encryption!

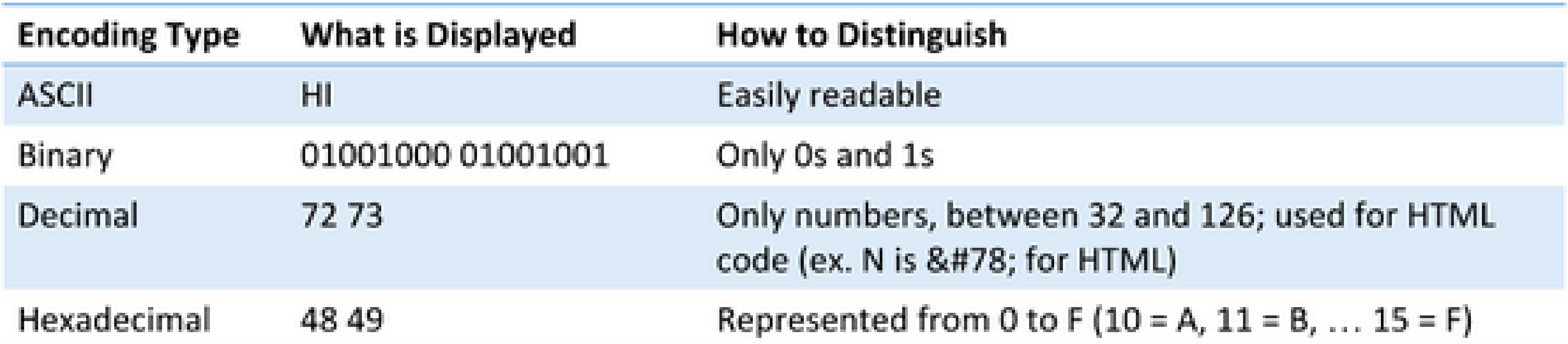
- Encoding is a reversible process, involving changing data to a new format using a specific scheme. Encoding is often done to convert data to a usable format for a specific purpose, but not usually to protect data as it is trivial to reverse.
- Encryption is also reversible – but can only be reversed by authorised users using a password or encryption key.
- Hence, whilst encryption DOES involve encoding, it is only used to refer to data that has been securely encoded in this manner.

Some Key Terms

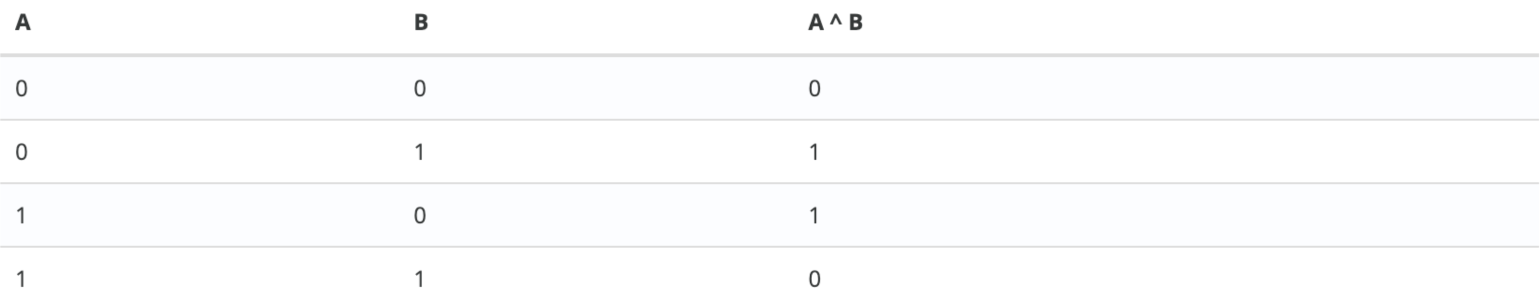
- **Plaintext** – Data before encryption, often in the form of text in the context of CTFs.
- **Ciphertext** – Data after encryption.
- **Brute force** – Attacking cryptography by trying every possible password or key.
- **Cryptanalysis** – Attacking cryptography by finding a weakness in an algorithm's underlying maths.

Let’s start!

XOR – Single Byte and Multibyte



Encoding Type	What is Displayed	How to Distinguish
ASCII	HI	Easily readable
Binary	01001000 01001001	Only 0s and 1s
Decimal	72 73	Only numbers, between 32 and 126; used for HTML code (ex. N is &#78; for HTML)
Hexadecimal	48 49	Represented from 0 to F (10 = A, 11 = B, … 15 = F)



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

XOR – continued

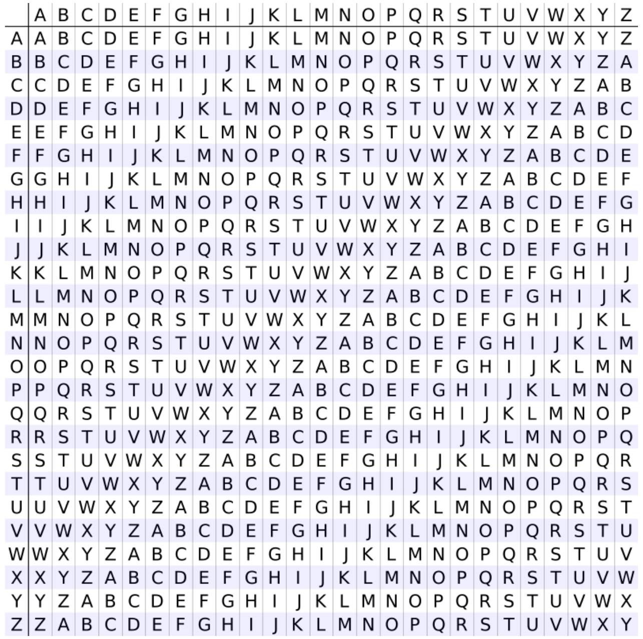
- Let’s do some decrypting together to demonstrate how things work in a CTF context:
- Key: A, which is 41 in Hex.
- We are given the ciphertext “boffe”, which is 62 6F 66 66 65 in Hex.
- You should have got the answer “hello”!

Simple Ciphers

- Ciphers are systems for encrypting or decrypting data. Some ciphers often count as encoding methods, but many aim to be solidly encrypted, ranging in complexity.
- Caesar Cipher – the simplest kind of cipher. Shift each letter in the plaintext by a given number to the next letter in the alphabet. Also sometimes known by ROT13, meaning rotate by 13 places in the alphabet, and includes variants ROT1 to ROT25.
- Substitution Cipher – similar in concept to Caesar, where each letter in plaintext is replaced by a different letter according to a given key. Caesar ciphers are technically a type of substitution cipher. Can often be cracked with frequency analysis, or a tool that I love called https://quipqiup.com/!

Harder Classical Ciphers…

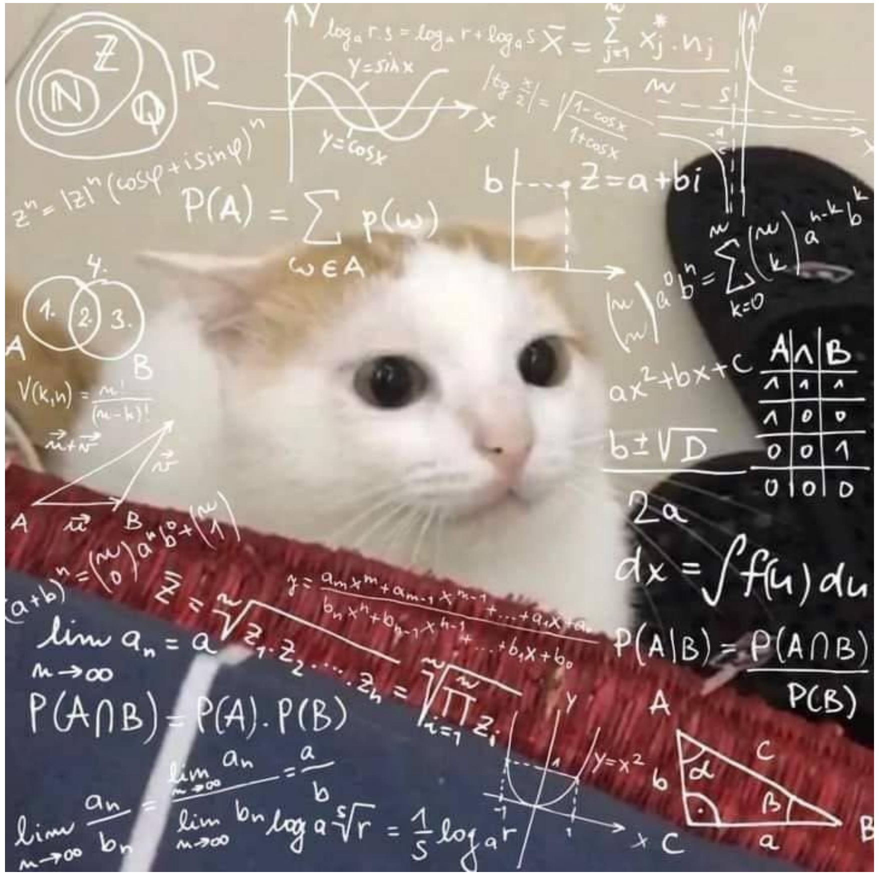
- Vigenere Cipher – still easily crackable with online tools, the Vigenere cipher is a Caesar cipher variant that uses a key. We pad out the key to the length of our plaintext, and then use each letter of the key as the row with our plaintext letter in the column within the table below, to find what letter to use in our ciphertext.



	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

- There are waaaay harder ciphers than Vigenere – this is really just the tip of the iceberg for classical cryptography!

Hashing Functions



- A hash function takes in an input of any size, and outputs a fixed-length summary, or "digest", of that data.
- A good hash function produces data that is hard to predict, and non-reversible – meaning you cannot get the input data from the output.
- Hashing functions often utilise modular arithmetic!
- Hence, theoretically, there are a set number of outputs for any hashing function. These can be placed in what we refer to as rainbow tables.

Hashing Functions – continued

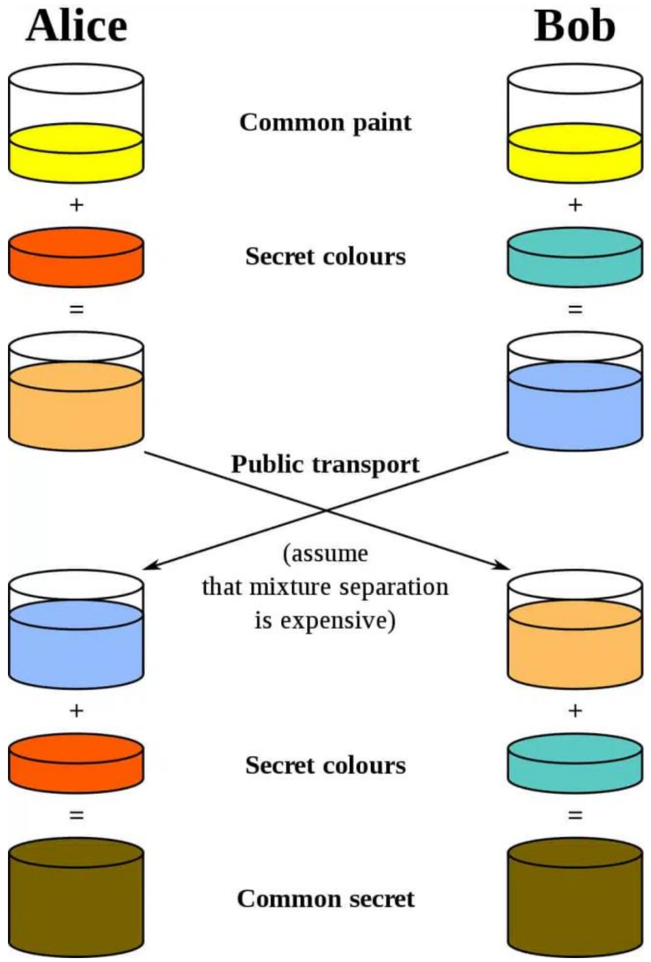
- In the context of CTFs, there are many hashing functions which have been proven insecure for various reasons.
- “In March 2005, Xiaoyun Wang and Hongbo Yu of Shandong University in China published an article in which they described an algorithm that can find two different sequences of 128 bytes with the same MD5 hash.”
- These attacks can even be used to create files with identical hashes!

Hashing Functions - Tools

- Commands like md5sum or shasum can help find hashes of files or strings in the Terminal.
- hashcat and John the Ripper are common tools used for attacking password hashes using rainbow tables.
- There are many online tools for checking for known hashes. Don't be afraid to try out new ones!

Oh no… maths…

Diffie-Hellman Key Exchange!



RSA

- An abbreviation of Rivest–Shamir–Adleman - who authored this cryptosystem!
- An implementation of asymmetric encryption that still holds up to this day – CTF challenges often involve exploiting poorly implemented RSA.
- RSA works on the idea that it is easy to generate a number by multiplying two sufficiently large prime numbers together…
- But factorising that number back into its original primes is extremely difficult and requires intense computational power. To add to this, RSA keys are often 1024 or 2048 bits in length.
- There are many attacks that can be done to find the plaintext if any of the numbers chosen to generate a ciphertext are too small or large in comparison to others.

Block ciphers and stream ciphers will be covered in a Term 2 cafe session – getting this content done is a session in itself!

But wait, there's something missing?

Things to Try!

- **Make an account at https://cryptohack.org/** - I cannot recommend this enough, it's the most comprehensive cryptography challenge resource out there with everything from basic ciphers to some very challenging encryption schemes!
- Or you can do some challenges on **PicoGym** for a taste of simpler cryptography across every discipline!

Tools and Resources

- RSACTFTool - https://github.com/Ganapati/RsaCtfTool
- CyberChef - https://cyberchef.io/
- dCode.fr - https://www.dcode.fr/tools-list#cryptography
- Crackstation (DON'T LAUGH IT'S USEFUL) - https://crackstation.net/
- Install PyCryptodome for Python – a lot of Crypto challenges involve scripting!