Cryptographic Attacks

References

- https://www.cryptool.org/en/
- https://github.com/hellman/xortool
- Cryptography E-Mates [Link]

Objectives

- Introduce a known-plaintext attack by attacking a monoalphabetic alphabet cipher with a letter frequency attack.

- Explore the impact of partially known plaintext through the disclosure of different file artifacts, including the header and null data.

Letter Frequency Attack

the congress, whenever two thirds of both houses shall deem it necessary, shall propose amendments to this constitution, or, on the application of the legislatures of two thirds of the several states, shall call a convention for proposing amendments, which, in either case, shall be valid to all intents and purposes, as part of this constitution, when ratified by the legislatures of three fourths of the several states, or by conventions in three fourths thereof, as the one or the other mode of ratification may be proposed by the congress; provided that no amendment which may be made prior to the year one thousand eight hundred and eight shall in any manner affect the first and fourth clauses in the ninth section of the first article; and that no state, without its consent, shall be deprived of its equal suffrage in the senate.

e	T	O	S	N	A	H	I	R	L	F	D	C	U	P	M	V	G	B	Y	W	Q
84	78	57	56	51	49	48	44	40	27	23	22	18	15	14	12	8	8	8	8	7	1

Letter Frequency Attack

the congress, whenever two thirds of both houses shall deem it necessary, shall propose amendments to this constitution, or, on the application of the legislatures of two thirds of the several states, shall call a convention for proposing amendments, which, in either case, shall be valid to all intents and purposes, as part of this constitution, when ratified by the legislatures of three fourths of the several states, or by conventions in three fourths thereof, as the one or the other mode of ratification may be proposed by the congress; provided that no amendment which may be made prior to the year one thousand eight hundred and eight shall in any manner affect the first and fourth clauses in the ninth section of the first article; and that no state, without its consent, shall be deprived of its equal suffrage in the senate.

E	T	O	S	N	A	H	I	R	L	F	D	C	U	P	M	V	G	B	Y	W	Q
84	78	57	56	51	49	48	44	40	27	23	22	18	15	14	12	8	8	8	8	7	1

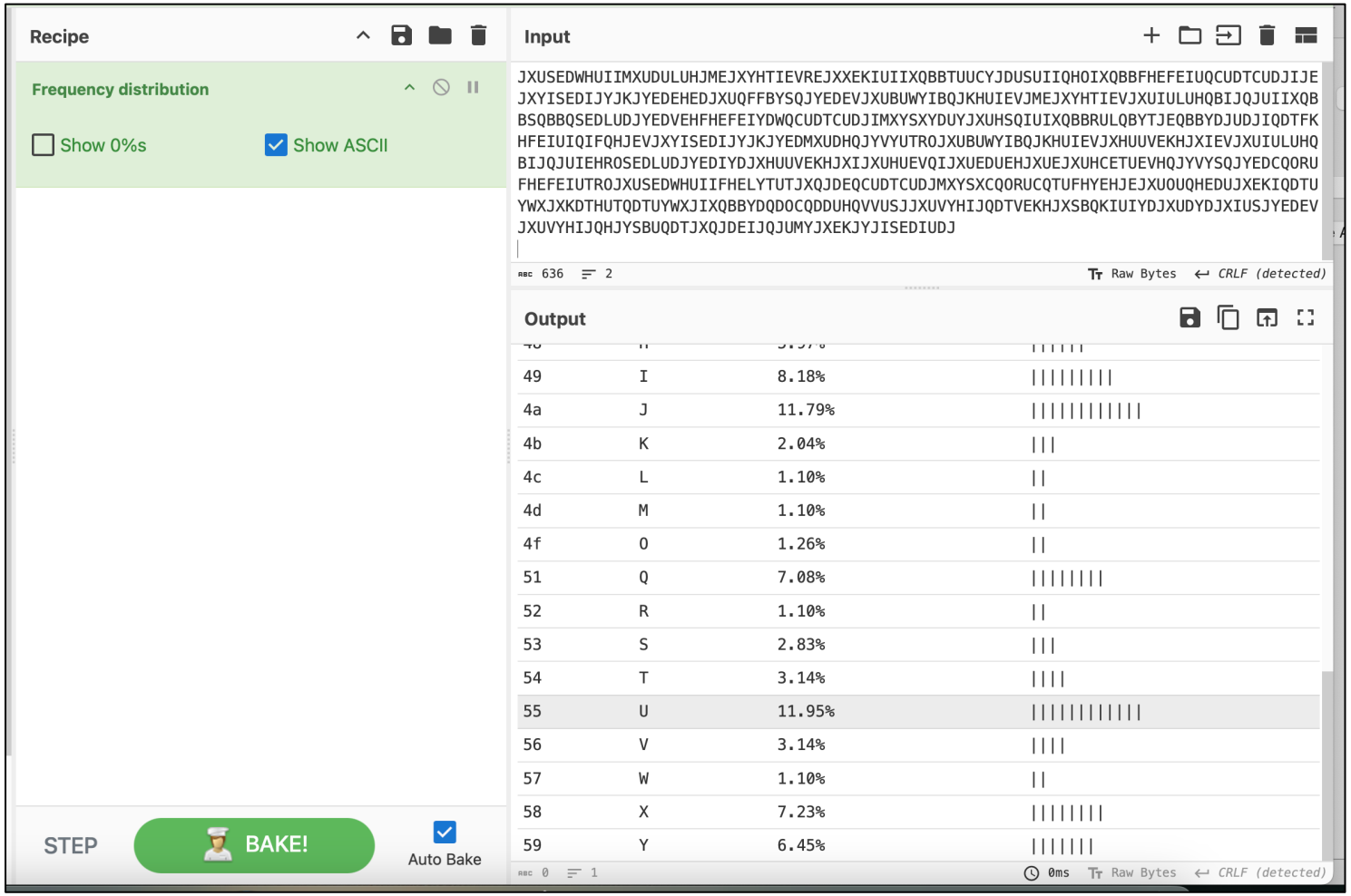
Letter Frequency Attack

```
>>>from pycipher import Caesar
>>>Caesar(key=-10).encipher('the
congress…')
```

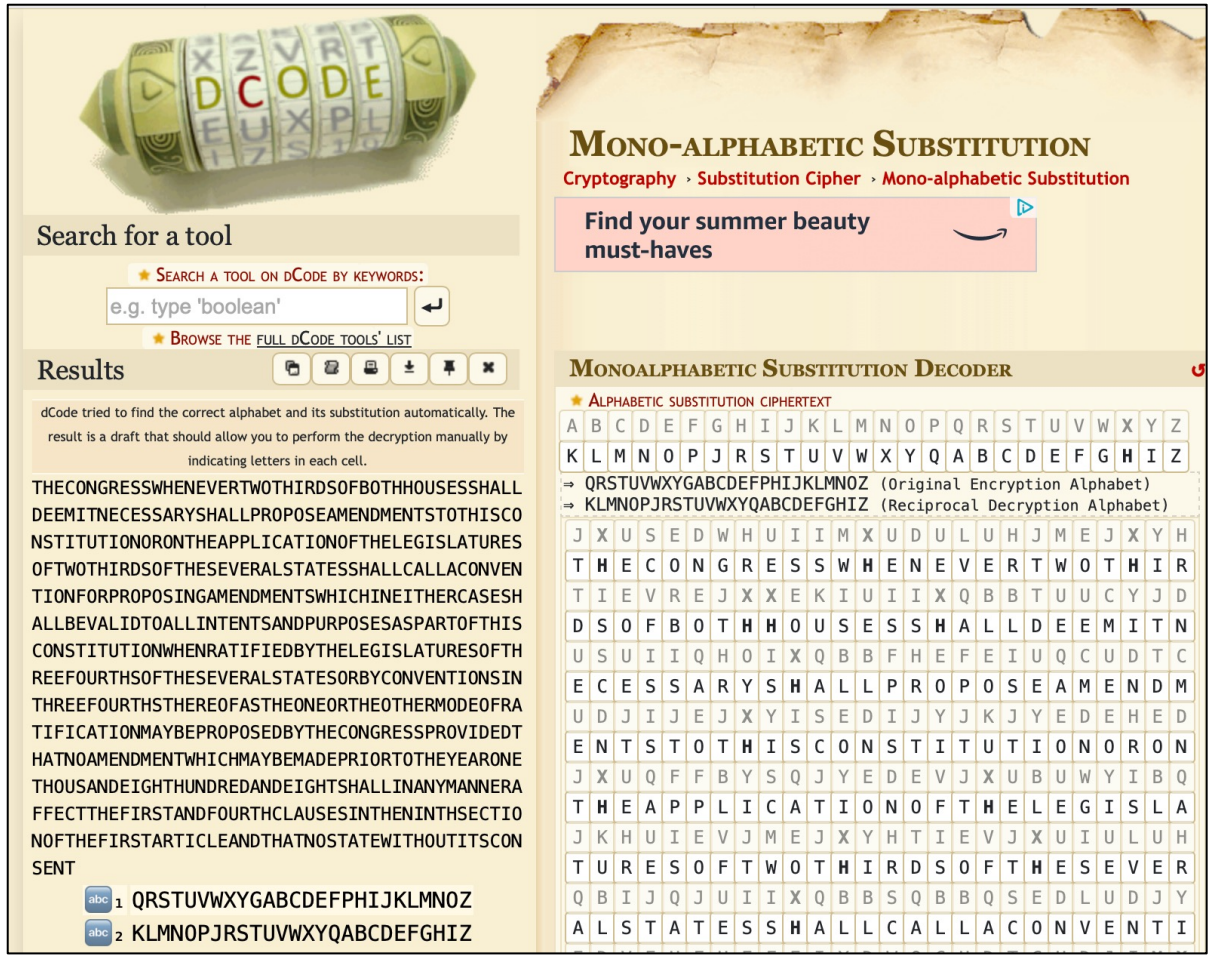
JXUSEDWHUIIMXUDULUHJMEJXYHTIEVREJXXEKIU
HEFEIUQCUDTCUDJIJEJXYISEDIJYJKJYEDEHEDJXU
IEVJMEJXYHTIEVJXUIULUHQBIJQJUIIXQBBSQBBQSEDLUDJYEDVEHFHEFEIYDWQCUDT
CUDJIMXYSXYDUYJXUHSQIUIXQBBRULQBYTJEQBBYDJUDJIQDTFKHFEIUIQIFQHJEVJX
YISEDIJYJKJYEDMXUDHQJYVYUTROJXUBUWYIBQJKHUIEVJXHUUVEKHJXIEVJXUIULUH
QBIJQJUIEHROSEDLUDJYEDIYDJXHUUVEKHJXIJXUHUEVQIJXUEDUEHJXUEJXUHCETUE
VHQJYVYSQJYEDCQORUFHEFEIUTROJXUSEDWHUIIFHELYTUTJXQJDEQCUDTCUDJMXY
SXCQORUCQTUFHYEHJEJXUOUQHEDUJXEKIQDTUYWXJXKDTHUTQDTUYWXJIXQBBYD
QDOCQDDUHQVVUSJJXUVYHIJQDTVEKHJXSBQKIUIYDJXUDYDJXIUSJYEDEVJXUVYHIJ
QHJYSBUQDTJXQJDEIJQJUMYJXEKJYJISEDIUDJ

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

CyberChef Frequency Analysis



Automating Frequency Analysis



- We can use tools like Dcode's Mono-alphabetic substitution to automatically solve ciphertext

- https://www.dcode.fr/monoalphabetic-substitution

Known Plaintext Attack

Remember our one-time pad cryptographic system

P = Plaintext

C = Ciphertext

K = Key

$C = P \oplus K$

```
>>> from pwn import *

>>> key='XYZ'
>>> xor('bABCDeFGHI',key)
b':\x18\x18\x1b\x1d\x1f\x1e\x1e\x12\x11'
```

Known Plaintext Attack

In this cryptosystem, we can recover K if we have P and C since:

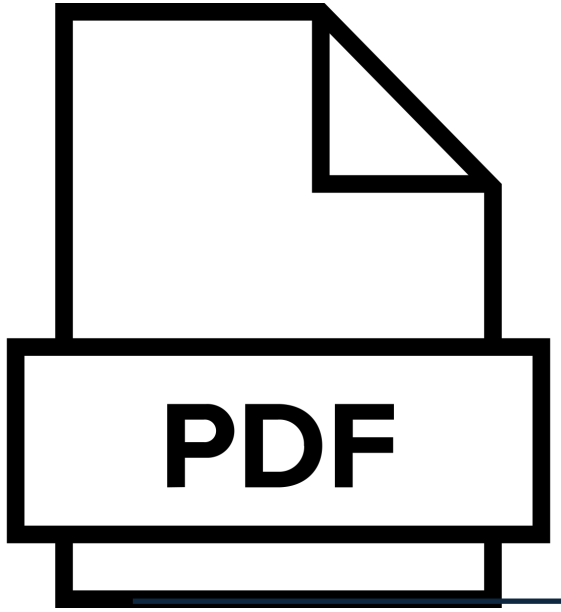
K = C ⊕ P

If we have a known start to a message like “ATTENTION”, and we know the key length is 3 we can recover the key by XOR(P[0:3],C[0:3])

P	A	T	T	E	N	T	I	O	N	:	A	T	T	A	C	K	T	O	D	A	Y
C	\x19	\r	\x0e	\x1d																	

```
>>> xor(b'ATT',b'\x19\r\x0e')
b'XYZ'
```

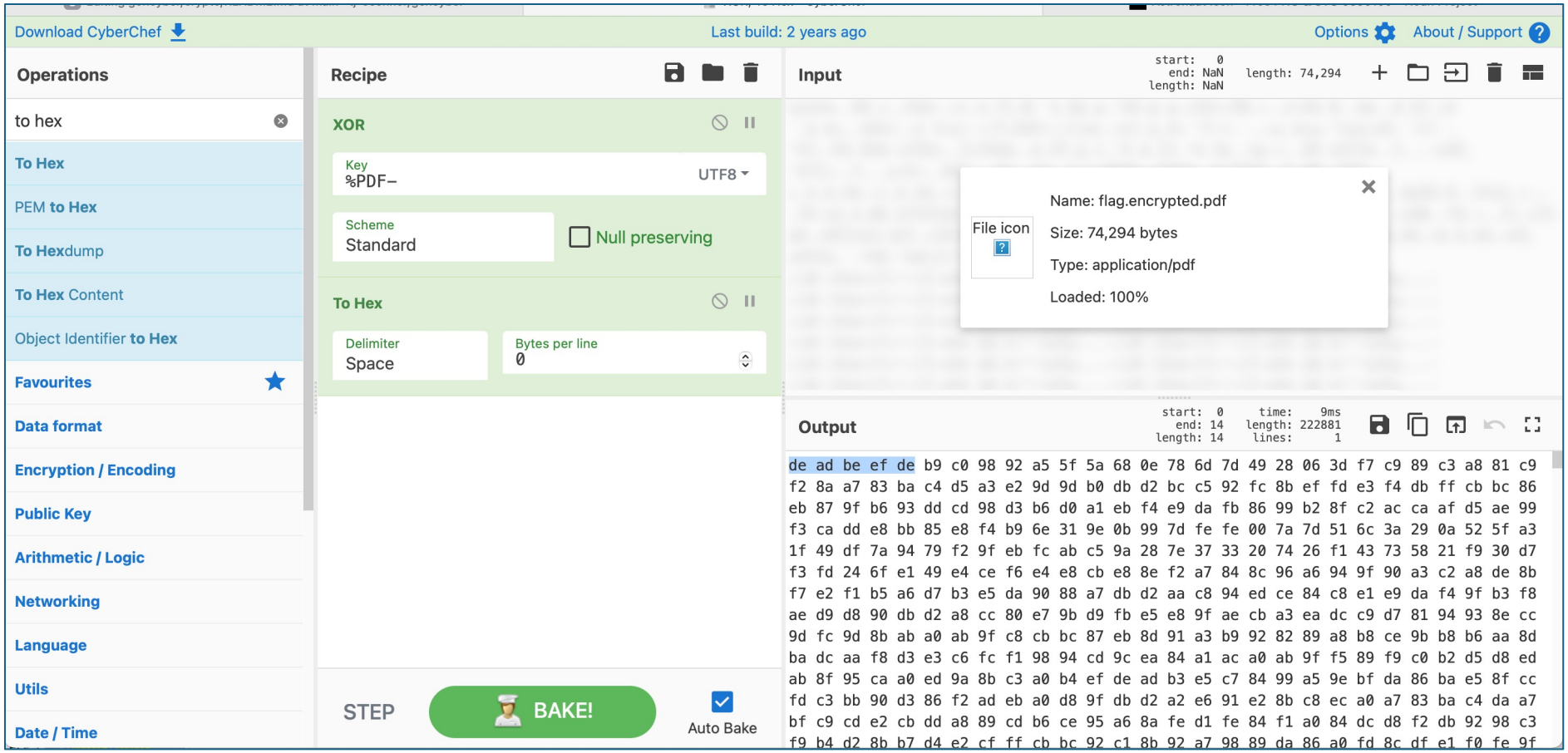
Known Plaintext Attack: Filetypes




```
{17:47}~/workspace ➪ hexdump -C flag.pdf | head -10
00000000  25 50 44 46 2d 31 2e 33  0a 25 c4 e5 f2 e5 eb a7  |%PDF-1.3.%......|
00000010  f3 a0 d0 c4 c6 0a 33 20  30 20 6f 62 6a 0a 3c 3c  |......3 0 obj.<<|
00000020  20 2f 46 69 6c 74 65 72  20 2f 46 6c 61 74 65 44  | /Filter /FlateD|
00000030  65 63 6f 64 65 20 2f 4c  65 6e 67 74 68 20 33 39  |ecode /Length 39|
00000040  36 20 3e 3e 0a 73 74 72  65 61 6d 0a 78 01 7d 52  |6 >>.stream.x.}R|
00000050  4d 4f 1b 31 10 bd ef af  78 a5 2d 5d 13 e2 8c c7  |MO.1....x.-]....|
00000060  df 57 68 0f 70 02 c9 12  07 e8 a1 5a 05 15 b4 29  |.Wh.p......Z...)|
00000070  4d d2 fe ff fa 23 5f 94  88 b5 64 7b 66 de bc 37  |M....#_...d{f..7|
00000080  eb 99 25 6e b1 44 40 f0  32 96 0f de 5b 19 19 46  |..%n.D@.2...[..F|
00000090  7b ac e6 b8 c3 2f cc 2e  d7 0a c3 1a aa ae f5 90  |{..../..........|
```

%	P	D	F	-	1	.	3													

Known Plaintext Attack: Filetypes



Known Plaintext Attack: Filetypes


```
{17:51}~/workspace ➪ hexdump -C flag | head -10
00000000  7f 45 4c 46 02 01 01 00  00 00 00 00 00 00 00 00  |.eLF............|
00000010  03 00 3e 00 01 00 00 00  40 10 00 00 00 00 00 00  |..>.....@.......|
00000020  40 00 00 00 00 00 00 00  e8 36 00 00 00 00 00 00  |@........6......|
00000030  00 00 00 00 40 00 38 00  0d 00 40 00 1e 00 1d 00  |....@.8...@.....|
00000040  06 00 00 00 04 00 00 00  40 00 00 00 00 00 00 00  |........@.......|
00000050  40 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00  |@.......@.......|
00000060  d8 02 00 00 00 00 00 00  d8 02 00 00 00 00 00 00  |................|
00000070  08 00 00 00 00 00 00 00  03 00 00 00 04 00 00 00  |................|
00000080  18 03 00 00 00 00 00 00  18 03 00 00 00 00 00 00  |................|
00000090  18 03 00 00 00 00 00 00  1c 00 00 00 00 00 00 00  |................|
```

eLF Files have a lot of null-byte (\x00) padding. We can take advantage of this. XOR encrypted binaries will often contain the key. Why?

C = P ⊕ K

C = \x00 ⊕ K = K

C = K

Helpful Information

CipherText = Plaintext $\oplus$ Key
PlainText = CipherText $\oplus$ Key

0x0 $\oplus$ Key = Key
0xff $\oplus$ Key = !Key