Mason Competitive Cyber

Cryptography

News since last meeting

- Equifax CEO Richard Smith “retires”
  - Massive Equifax Hack exposing a ton of PII

- Verizon accidentally exposed data on S3
  - Server logs
  - Credentials

- nRansomware
  - Send nudes instead of bitcoin

Upcoming CTFs & Events

- Sam (of Kudu Dynamics) on CSAW CTF 2017 problems
  - Guest speaking
  - Now
  - Johnson Center Meeting Room G

- DefCamp CTF Quals
  - September 30 8am to October 1, 8am
  - Online

- Capital One Wargame
  - October 3, 6pm to 9pm
  - 1680 Capital One Drive, McLean VA
  - In-person
  - teams?

Cryptography

- Way of securing information so it’s only readable by intended recipient

- Category in almost every CTF
  - Simple ciphers
  - Related: steganography
  - XOR
  - RSA

Terms

- Plaintext, sometimes called clear text (p) = the message
- Ciphertext (c) = the disguised message
- Encrypt = plaintext -> ciphertext
- Decrypt = ciphertext -> plaintext
- Key (k) = in symmetric crypto, information needed to encrypt and/or decrypt

Codes

- Codes are made to present information differently, not meant to be secure
  - Binary 0 1
  - Morse . -
  - Hex 0-1 a-f
  - Base64 length divisible by 4, sometimes has “=” at the end

- In medium difficulty problems, could be multiple codes/ciphers

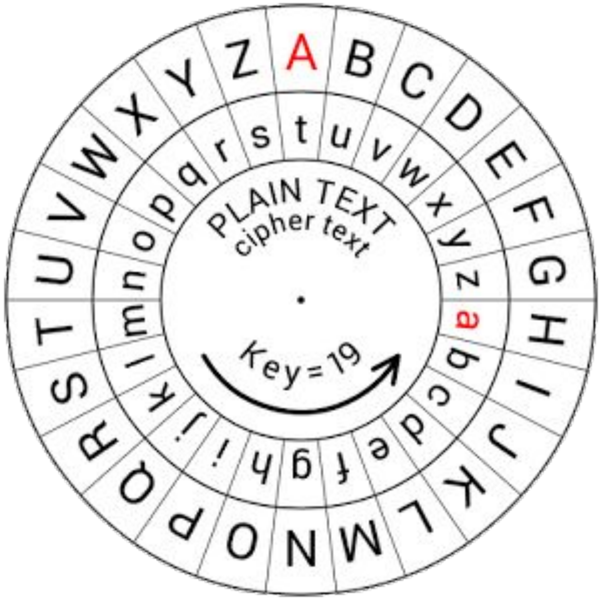
- In harder problems, data is often hex encoded

Simple Ciphers

- Ciphertool.py
  - Our tool to solve simple ciphers
  - On our github

- Caesar
  - Rotate letters in alphabet
  - a->c b->d c->e

- Breaking Caesar
  - Brute force (try all combinations) - 25
  - ciphertool


PLAIN TEXT
cipher text
Key = 19
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 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

Simple Ciphers

- Substitution cipher
  - Like caesar except no rotation
  - Pick randomly which letters to substitute

    a->z b->c

- Breaking substitution
  - can’t brute force
  - frequency analysis
  - quipqiup

XOR

⊕

- Exclusive OR
- Used in One Time Pad (OTP)
  - p⊕k = c
  - c⊕k = p
  - Theoretically impossible to crack
  - Impractical

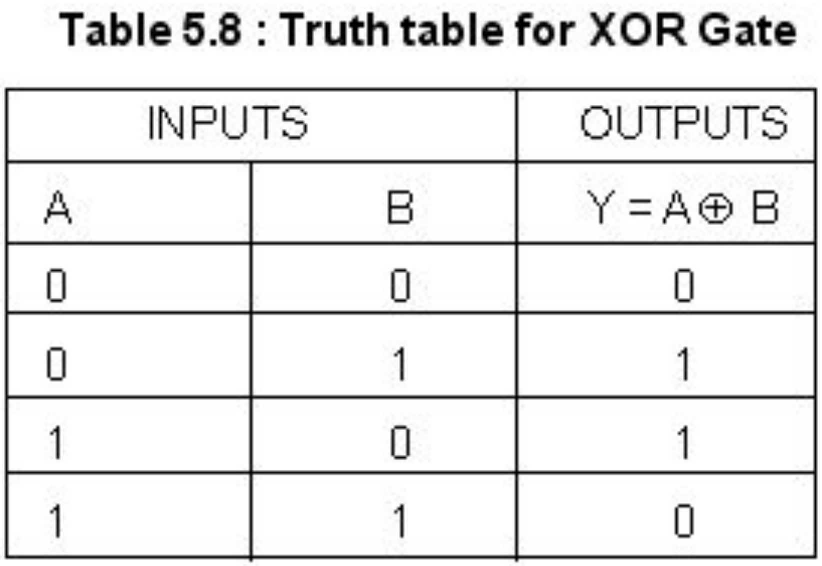


Table 5.8 : Truth table for XOR Gate

INPUTS		OUTPUTS
A	B	Y = A⊕ B
0	0	0
0	1	1
1	0	1
1	1	0

Super Fast Binary Refresher

- Bit = 0 or 1
- Byte = 8 bits

Binary	**Decimal**
00000000	0
00000001	1
00000010	2
00000100	4
00000011	3
00000101	5
11111111	255

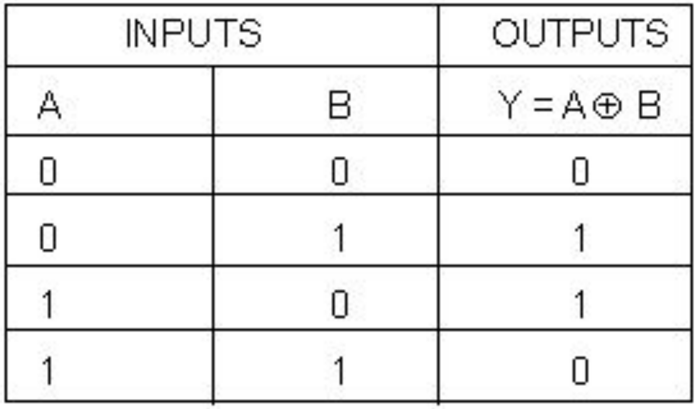
Single Bit XOR

- Bit = 0 or 1
- Byte = 8 bits
- Key repeats if shorter than the message

- Single bit XOR (with k=1)
  p: MCC
  p: 01101101 01100011 01100011
  k: 11111111 11111111 11111111
  c: 10010010 10011100 10011100

  $p \oplus k = c$

Table 5.8 : Truth table for XOR Gate



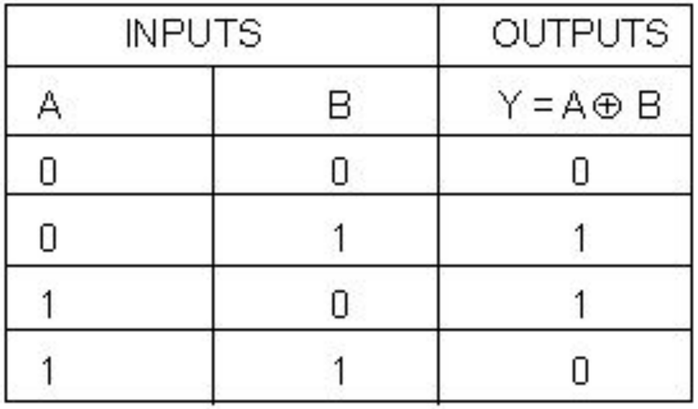
INPUTS		OUTPUTS
A	B	$Y = A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

Single Bit XOR

- Breaking single bit XOR
  c: 10010010 10011100 10011100

  $p \oplus k = c$
  $c \oplus k = p$

Table 5.8 : Truth table for XOR Gate



INPUTS		OUTPUTS
A	B	Y = A ⊕ B
0	0	0
0	1	1
1	0	1
1	1	0

Breaking Single Bit XOR

- Since key is a bit, and bit can only be 0 or 1, brute force by trying k=0 and k=1

  c: 10010010 10011100 10011100
  k: 00000000 00000000 00000000
  p: 10010010 10011100 10011100
  p: &#8217;&#339;&#339;

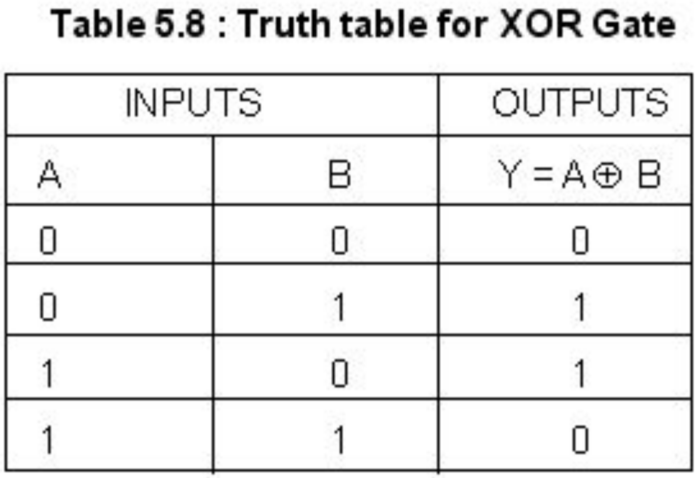


Table 5.8 : Truth table for XOR Gate

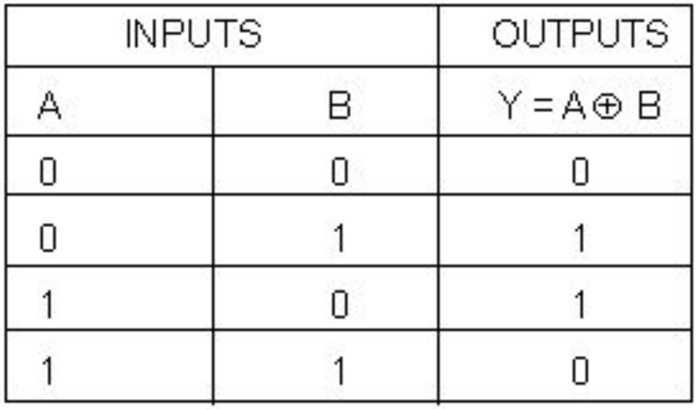
INPUTS		OUTPUTS
A	B	Y = A ⊕ B
0	0	0
0	1	1
1	0	1
1	1	0

Breaking Single Bit XOR

- Since key is a bit, and bit can only be 0 or 1, brute force by trying k=0 and k=1

  c: 10010010 10011100 10011100
  k: 11111111 11111111 11111111
  p: 01101101 01100011 01100011
  p: MCC

Table 5.8 : Truth table for XOR Gate



INPUTS		OUTPUTS
A	B	Y = A ⊕ B
0	0	0
0	1	1
1	0	1
1	1	0

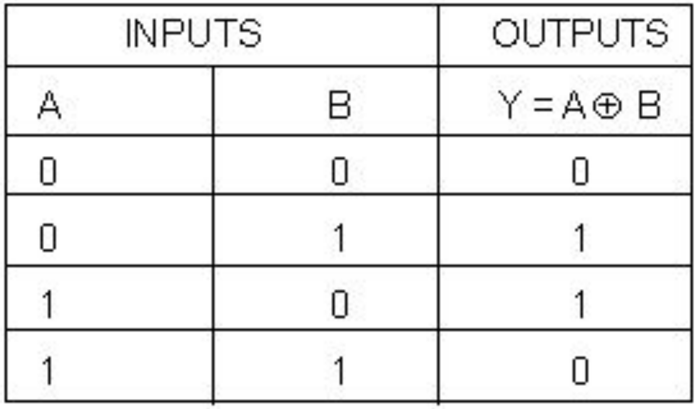
Single Byte XOR

- Byte = 8 bits
- Bit = 0 or 1
- Key repeats if shorter than the message

- Single byte XOR (with k=29)
  p: MCC
  p: 01101101 01100011 01100011
  k: 00011101 00011101 00011101
  c: 01110000 01111110 01111110

  $p \oplus k = c$

Table 5.8 : Truth table for XOR Gate



INPUTS		OUTPUTS
A	B	$Y = A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

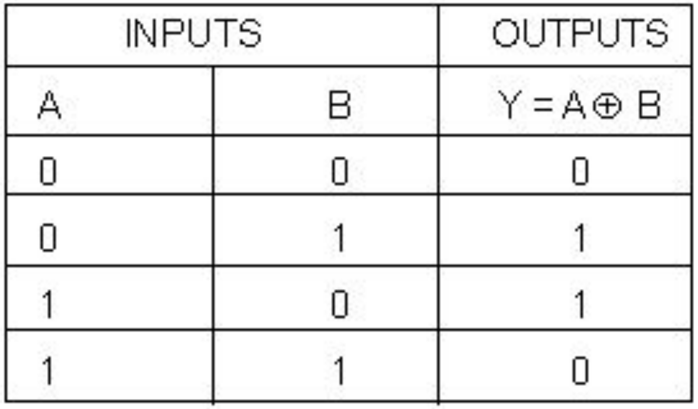
Breaking Single Byte XOR

- Byte = 8 bits
  - 255 possible keys

- Single byte XOR
  c: 01110000 01111110 01111110

  c⊕k = p

Table 5.8 : Truth table for XOR Gate



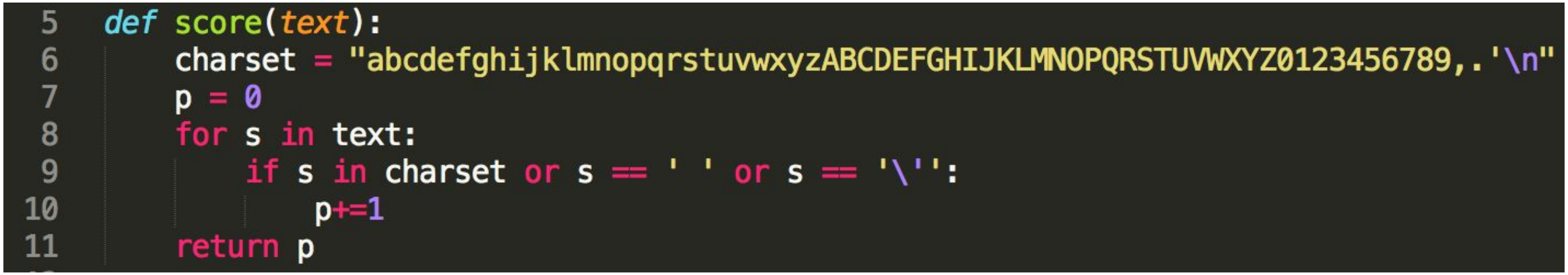
INPUTS		OUTPUTS
A	B	$Y = A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

Breaking Single Byte XOR

- Byte = 8 bits
  - 255 possible keys

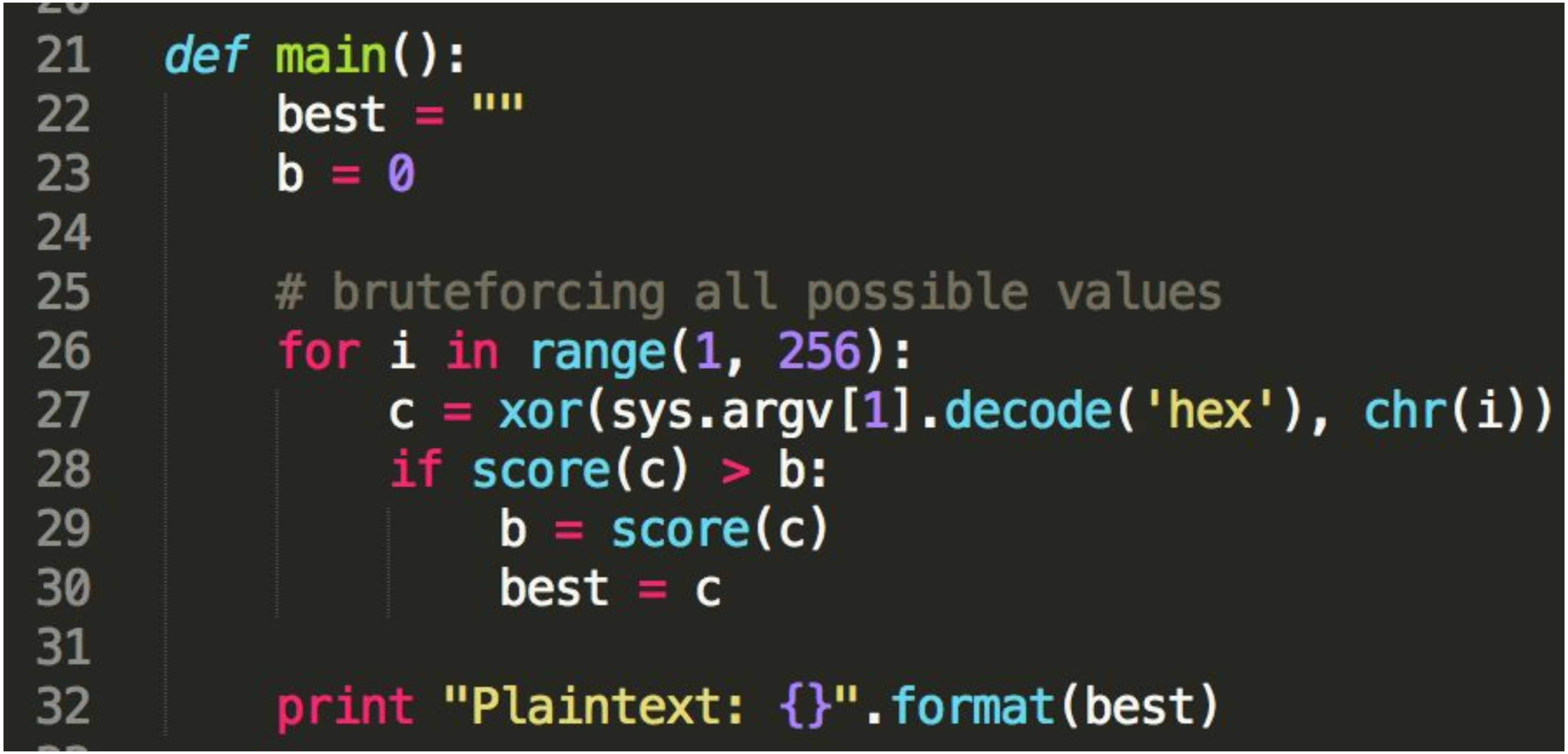
- Single byte XOR
  c: 01110000 01111110 01111110

- Brute force (try all 255)
- Score plaintexts
  - Can’t search for “ctf” or “flag”
  - Score = how many valid characters in p



```
def score(text):
    charset = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789,.'\n"
    p = 0
    for s in text:
        if s in charset or s == ' ' or s == '\'':
            p+=1
    return p
```

Breaking Single Byte XOR



```
def main():
    best = ""
    b = 0

    # bruteforcing all possible values
    for i in range(1, 256):
        c = xor(sys.argv[1].decode('hex'), chr(i))
        if score(c) > b:
            b = score(c)
            best = c

    print "Plaintext: {}".format(best)
```

Challenges

- go.gmu.edu/basic 4
- Training CTF
  - Up all the time from now on
  - t2.micro instance (read: slow)
  - go.gmu.edu/tctf
  - flag format: masoncc{flag}

Proud Sponsors

Thank you to these organizations who give us their support: