CodePath

Week 5

CS 4760 F18
Christopher Raley

Codepath Homework

CTF Homework by 10/7 @ 11:59 PM

- Including extra credit

Topics

Week 5

Readings on course website

Discussed in detail in future lectures

- Simple Ciphers
- Symmetric-Key Algorithms
- Public-Key Cryptography
- Cryptographic Hash Algorithms
- Checksums
- Password Hashing

Encryption

- **Encryption** is the process of transforming information to keep it private so that only a select few individuals are able to decode it
  - Note that **encoding** is just the transferring of data into another format
- Result of encryption is **ciphertext**
  - This results when plaintext is used as input for some encryption algorithm
    - Example: 3DES, AES

Shift Ciphers

- **Shift Cipher -** The method to encrypt is to take each character of a message and shift it a certain number of characters to the left or right.
  - Example: Caesar Cipher (used a shift of 3)

- **ROT13** - One of the more popular shift ciphers. Shifts letters 13 positions (half of the alphabet)

ROT13 Example

Guvf vf n frperg zrffntr

Substitution Ciphers

- **Substitution Cipher -** Uses a translation map for characters, so that each character in the text gets translated into another character
  - Substitutions can be completely random
  - Example:
    - ‘ABCDEFGHIJKLMNOPQRSTUVWXYZ’
    - ‘UMRSQPBOLEXTZYAKJVCNHDWGIF’
  - Vulnerability?

Letter	Relative frequency in the English language
a	8.167%
b	1.492%
c	2.782%
d	4.253%
e	12.702%
f	2.228%
g	2.015%
h	6.094%
i	6.966%
j	0.153%
k	0.772%
l	4.025%
m	2.406%
n	6.749%
o	7.507%
p	1.929%
q	0.095%
r	5.987%
s	6.327%
t	9.056%
u	2.758%
v	0.978%
w	2.360%
x	0.150%
y	1.974%
z	0.074%

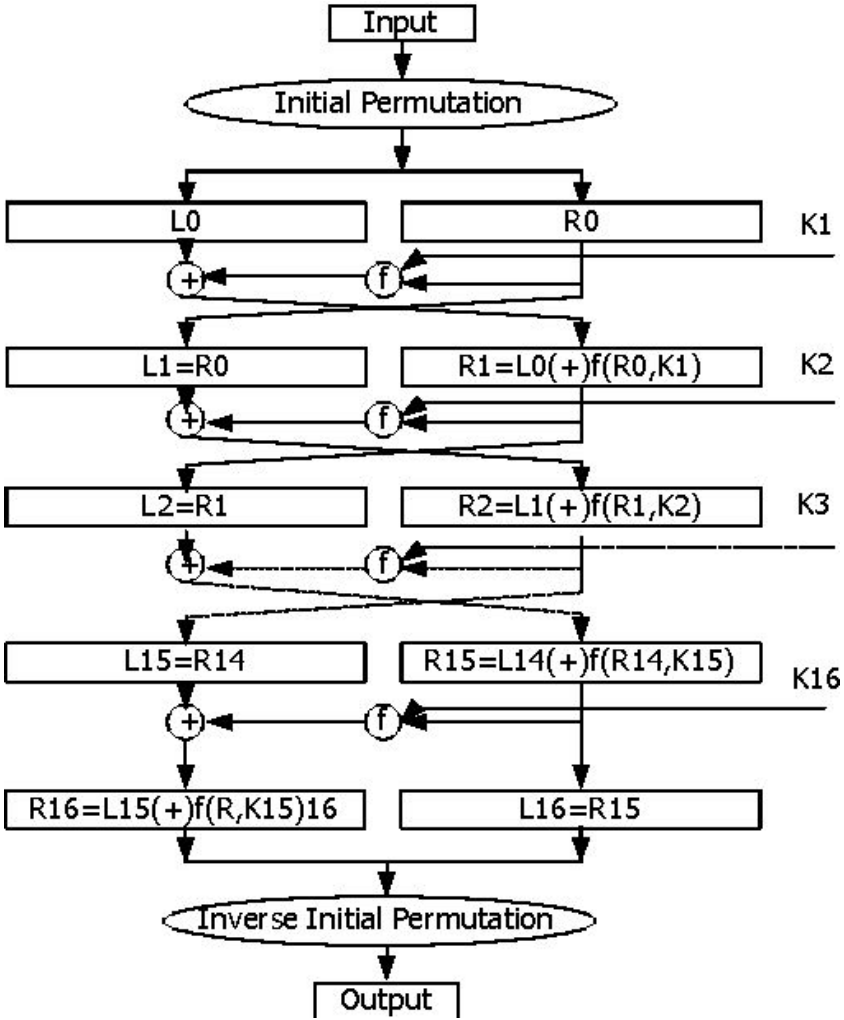
“TO BE OR NOT TO BE”

NA MQ AV YAN NA MQ

Symmetric Key Algorithms

- **Symmetric-Key Algorithm -** Uses a string of data to encrypt and decrypt information
  - Think of lock and and key situation
  - This string of data can reverse an an algorithms output so that we get the original plaintext (via mathematical properties)

- Problem lies in how exactly do you securely transfer those keys


Input
Initial Permutation
L0
R0
K1
+
f
L1=R0
R1=L0(+)f(R0,K1)
K2
+
f
L2=R1
R2=L1(+)f(R1,K2)
K3
+
f
L15=R14
R15=L14(+)f(R14,K15)
K16
+
f
R16=L15(+)f(R,K15)16
L16=R15
Inverse Initial Permutation
Output

Cryptographic Hash Algorithms

- **Cryptographic Hash Algorithms -** One-way algorithms (extremely difficult to invert output back into original input) that produce **checksums.**
  - Examples: MD5, SHA, bcrypt
  - Used for **integrity**
  - Hopefully used for producing hashed passwords

- You will commonly find websites that have downloads show a MD5 hash for you to compare to...

MD5 Example

“Hello World!”

ed076287532e86365e841e92bfc50d8c

MD5 Example

“Hello World”

b10a8db164e0754105b7a99be72e3fe5

MD5 Example

ed076287532e86365e841e92bfc50d8c

b10a8db164e0754105b7a99be72e3fe5

CTF Tips

- Some challenges require Burp
- Make use of online resources
  - https://www.dcode.fr/xor-cipher
  - https://www.base64decode.org/
  - https://cryptii.com/pipes/caesar-cipher
- Try writing code to decrypt things for you
  - Useful for brute forcing

Office Hours

Monday / Thursday / Sunday : 5 - 7 PM @ Rice 226