CSE 484 / CSE M 584
Computer Security

TA: Jared Moore
jlcmoore@cs
Logistics

• Lab #1 due next Friday

• Today:
  – Lab 1 questions.
  – Authentication grab bag.
  – (if time) Cryptography
Password Salting

• Servers shouldn’t store passwords, but password hashes. (Why?)
• Threat: rainbow tables (pre-computed password hashes)
• Solution: salt
  – Each password is hashed/stored with a random value. Now a pre-computed table is useless.
  – Other benefits?
Measuring Password Strength

• How many possible passwords are there?
• How many passwords are likely to be chosen?
• How long will it take to guess?

• Bits of entropy: $\log_2(\text{# of guesses})$

Example: password of 10 bits chosen randomly
Possible passwords = $2^{10}$
Bits of entropy = $\log_2(2^{10}) = 10$

Additional bit of entropy doubles number of guesses needed.
Password Meters

[From “How does your password measure up? The Effect of Strength Meters on Password Creation”, Ur et al., USENIX Security 2012]
Password Meters

• Meters lead to longer passwords.
• Are passwords harder to guess?
  – Visual feedback alone has no effect.
  – More stringent meters do lead to stronger passwords.
• Meters lead to people taking longer to create passwords, and change their mind during creation.
• Meters don’t affect memorability.

[From “How does your password measure up? The Effect of Strength Meters on Password Creation”, Ur et al., USENIX Security 2012]
Usable Two-Factor Authentication

• Use phone as a second factor automatically.

• What if phone is not present?
  – Server can treat login session differently (e.g., don’t allow transactions above a threshold $ amount).

[From “Strengthening User Authentication through Opportunistic Cryptographic Identity Assertions”, Czeskis et al., CCS 2012]
Cryptography
Caesar Cipher (Shift Cipher)

- Plaintext letters are replaced with letters a fixed shift away in the alphabet.

- Example:
  - Plaintext: The quick brown fox jumps over the lazy dog.
  - Key: Shift 3
    
    ABCDEFGHIJKLMNOPQRSTUVWXYZ
    DEFGHIJKLMNOPQRSTUVWXYZABC

  - Ciphertext: WKHTX LFNEU RZQIR AMXPS VRYHU WKHOD CBGRJ
Caesar Cipher (Shift Cipher)

• ROT13: shift 13  (encryption and decryption are symmetric)

• What is the key space?
  – 26 possible shifts.

• How to attack shift ciphers?
  – Brute force.
Substitution Cipher

• Superset of shift ciphers: each letter is substituted for another one.

• **Monoalphabetic substitution cipher**: fixed substitution over the entire message.

• Example:
  - Plaintext: **ABCDEFGHIJKLMNOPQRSTUVWXYZ**
  - Cipher: **ZEBRASCDFGHIJKLMNOPQRSTUVWXYZ**
  - Cipher: **ZEBRASCDFGHIJKLMNOPQRSTU**
Substitution Cipher

• What is the key space? 26! \(\sim 2^{88}\)

• How to attack?
  – Frequency analysis.

Bigrams:

- th 1.52%
- he 1.28%
- in 0.94%
- er 0.94%
- an 0.82%
- re 0.68%
- nd 0.63%
- at 0.59%
- on 0.57%
- nt 0.56%
- ha 0.56%
- es 0.56%
- st 0.55%
- th 1.52%
- he 1.28%
- in 0.94%
- er 0.94%
- an 0.82%
- re 0.68%
- nd 0.63%
- at 0.59%
- on 0.57%
- nt 0.56%
- ha 0.56%
- es 0.56%
- st 0.55%

Trigrams:

1. the 6. ion 11. nce
2. and 7. tio 12. edt
3. tha 8. for 13. tis
4. ent 9. nde 14. oft
5. ing 10. has 15. sth
Transposition Cipher

• Ciphertext is permutation of plaintext.
• Example: **Route cipher**
  - Plaintext: *WE ARE DISCOVERED, FLEE AT ONCE*
  - Arrangement:
    - W R I O R F E O E
    - E E S V E L A N J
    - A D C E D E T C X
  - Key: “spiral inwards, clockwise, starting from top right”
  - Ciphertext: **EJXCTEDDECDAEWRIORFEONALEVSE**
What is this?

Scytale
(used by ancient Greeks/Spartans)

How is it used to do transposition?

1. Wrap
2. Write horizontally
3. Encrypt = unwrap
4. Decrypt = rewrap
Transposition/Substitution

• How to tell if ciphertext was encrypted using substitution or transposition cipher?
  – If letter frequencies are normal, it’s transposition.

• What happens if you combine substitution and transposition?
  – Substitution prevents anagram finding, transposition prevents digram/trigram analysis.
Vigenère Cipher (~1467)

- Polyalphabetic substitution cipher: use multiple substitution alphabets.
- Example:
  - Plaintext: ATTACKATDAWN
  - Key: LEMONLEMONLE
  - Ciphertext: LXFOPVEFRNHR
- Encrypt:
  - (Key-Row, Msg-Col)
  - Or just addition mod 26
Vigenère Cipher (~1467)

• Does this defeat frequency analysis?
  – Not if you know the length of the (repeating) key (e.g., if key length = 5, do frequency analysis on set of every 5th letter).
  – Even if you don’t know the key length, just iterate with length=1...n until decryption looks sensible.

• What if the key doesn’t repeat (i.e., length of key >= length of plaintext)?
  – One-time pad. (Same caveats: fully random key, use only once...
Steganography

- Hidden messages (security through obscurity)

Figure 1. Modern steganographic communication. The encoding step of a steganographic system identifies redundant bits and then replaces a subset of them with data from a secret message.

[Figure from “Hide and Seek: An Introduction to Steganography” by Niels Provos and Peter Honeyman]
Block Cipher Mode: ECB
Block Cipher Mode: CBC

[Figure from Yoshi’s slides]
Block Cipher Mode: CTR

Initial $\text{ctr}$ (random) → $\text{ctr}$, $\text{ctr}+1$, $\text{ctr}+2$, $\text{ctr}+3$ → $\text{block cipher}$ → $\text{ct}$ → $\text{ciphertext}$

[Figure from Yoshi’s slides]