说说口令安全这件事

复旦大学 韩伟力

What are passwords?

“

A password is a word or string of characters used for user authentication to prove identity or access approval to gain access to a resource (example: an access code is a type of password), which is to be kept secret from those not allowed access.

”

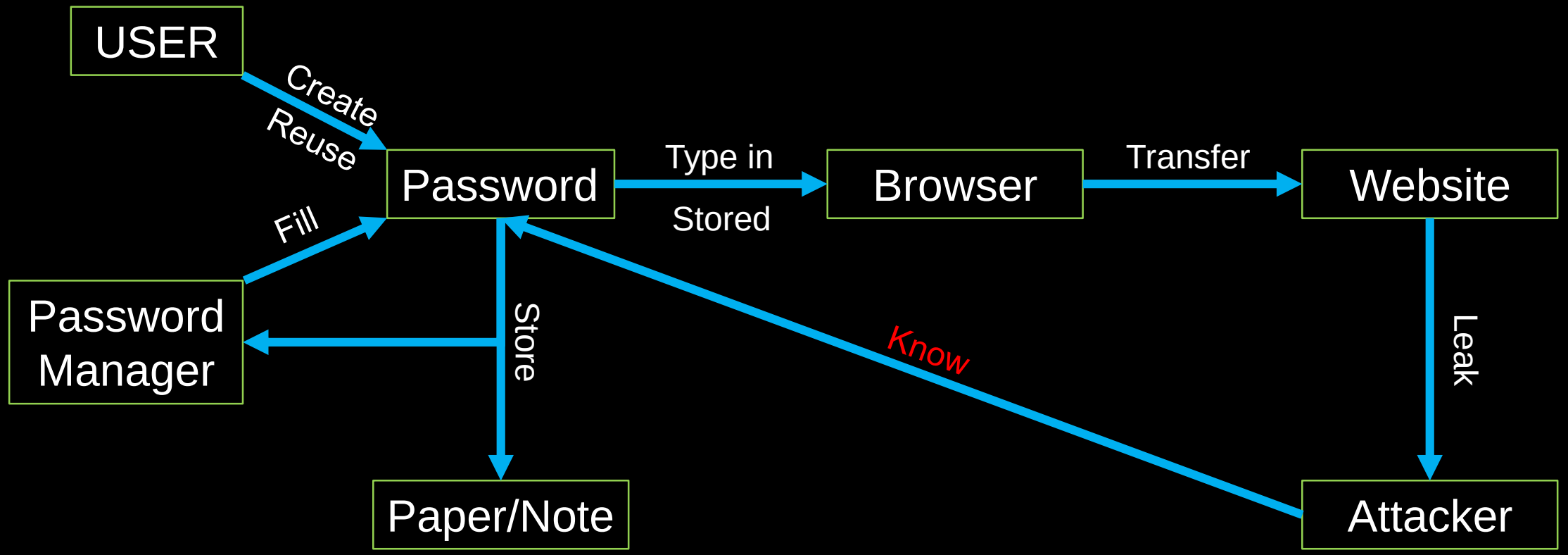
https://en.wikipedia.org/wiki/Password

Motivation to Study Passwords

- Important of Passwords
- Vulnerabilities of Password-based Authentication
- Science of Security

Life Cycle of Passwords

Life Cycle of Passwords



Password Guessing

Password Guessing

- **Dictionary Guessing**

  Use popular passwords, with mangling rules.

- **Brute-force Guessing**

  Search all the password space.

Dictionary Guessing——John the Ripper

Jack the Ripper is the best known name given to an unidentified serial killer generally believed to have been active in the largely impoverished areas in and around the Whitechapel district of London in 1888.

https://en.wikipedia.org/wiki/**Jack_the_Ripper**

Dictionary Guessing——PCFG-based Method

- **Matt Weir *et al*：**
  ***Password Cracking Using Probabilistic Context-Free Grammars*.**

- **Input:**
  - **Dictionary**
  - **Training Set**

Dictionary Guessing——PCFG-based Method

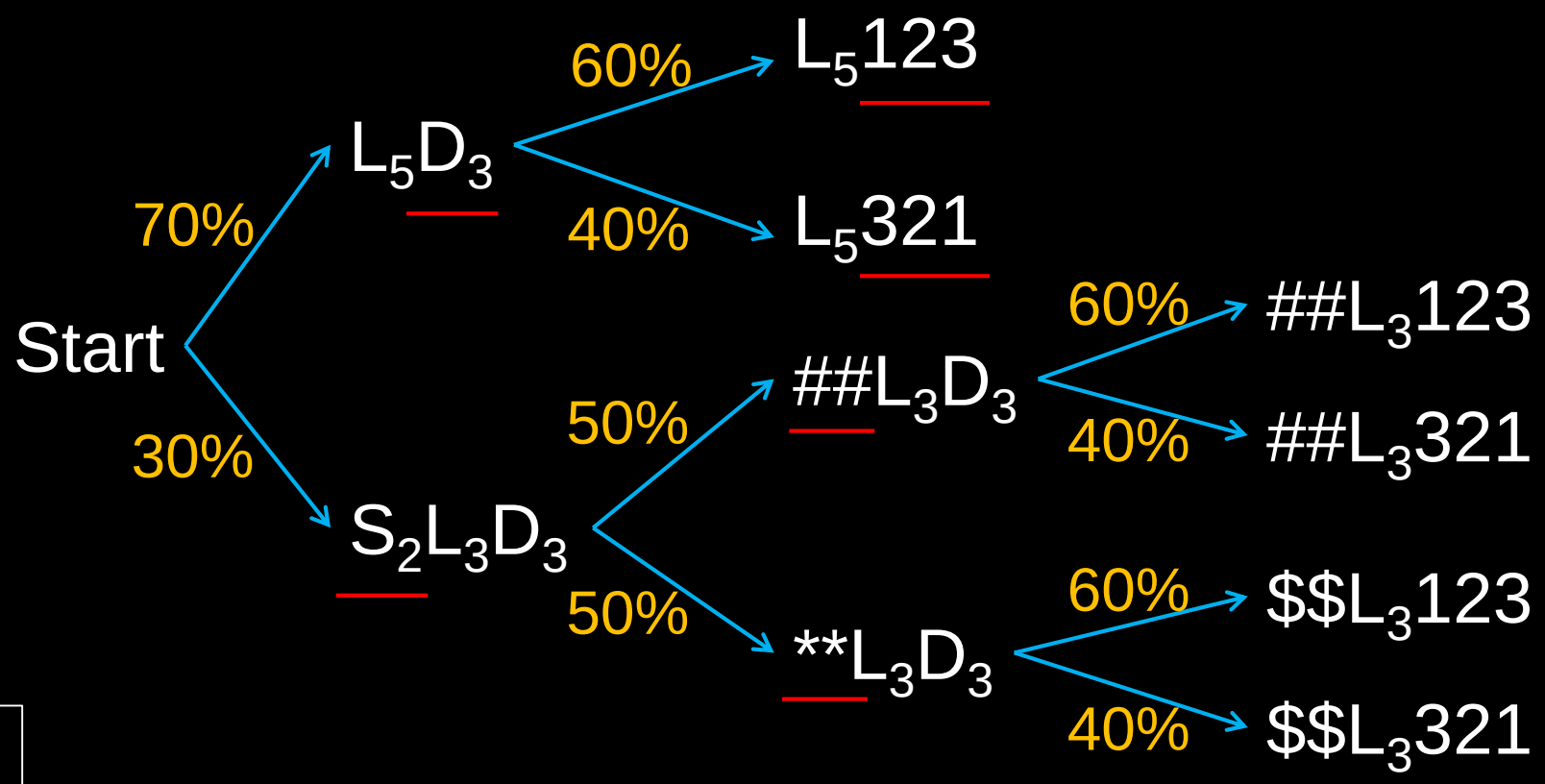
Training Set

*password, admin123, 123456, ##hello***

$S \to L_8$	25%	$D_3 \to 123$	100%
$S \to L_5D_3$	25%	$D_6 \to 123456$	100%
$S \to D_6$	25%	$S_2 \to ##$	50%
$S \to S_2L_5S_2$	25%	$S_2 \to **$	50%

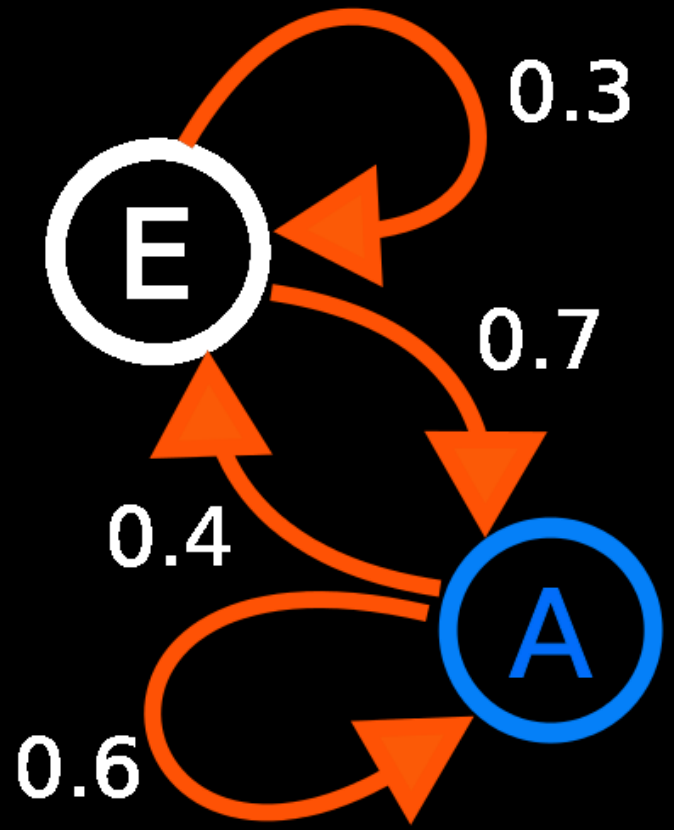
For letters, using a dictionary.

Dictionary Guessing——PCFG-based Method



L_n = n letters
D_n = n digits
S_n = n symbols

Brute-Force Guessing——Markov Model

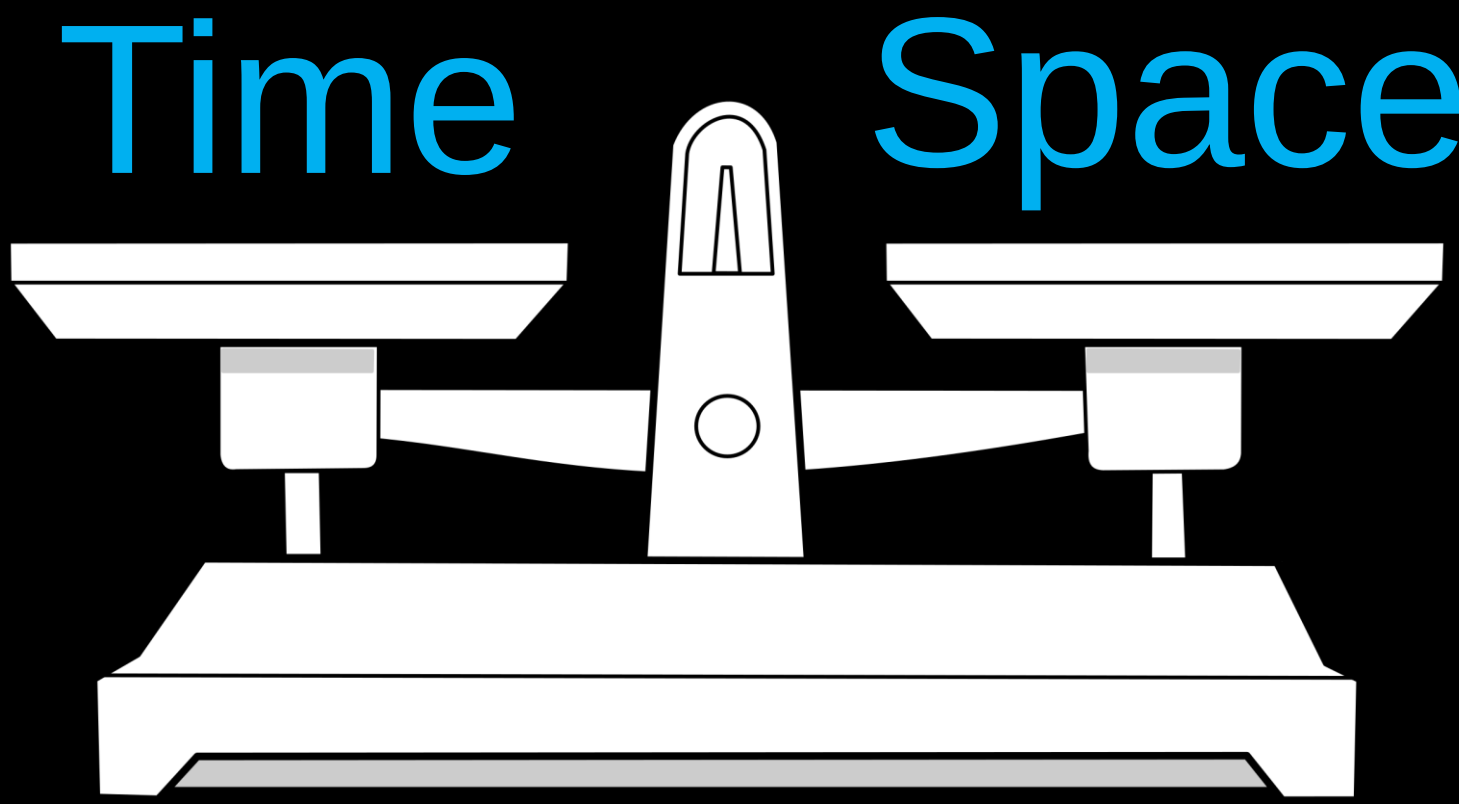


Order-1

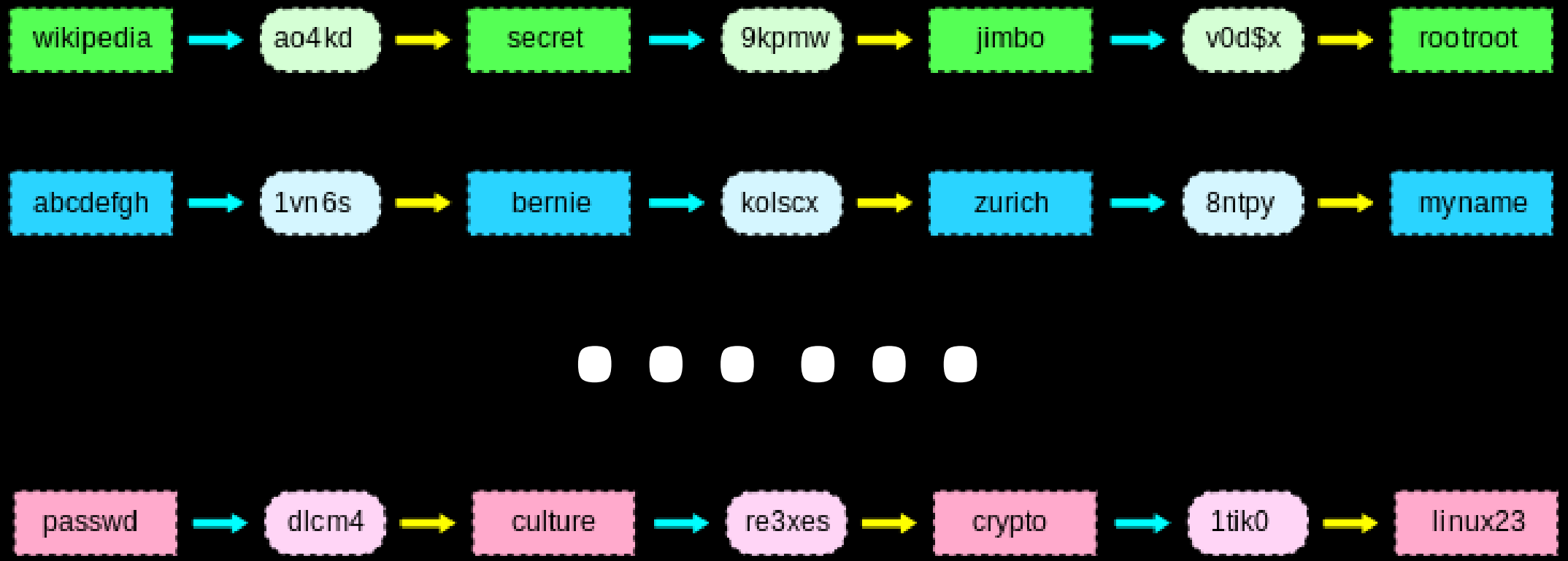
$$P(c_1 c_2 \dots c_n) = P(c_1|c_0 c_0)P(c_2|c_0 c_1)P(c_3|c_1 c_2) \dots P(c_n|c_{n-2} c_{n-1})$$

Order-2

Brute-Force Guessing——Rainbow Table



Brute-Force Guessing——Rainbow Table



Graphic Passwords

Graphic Passwords

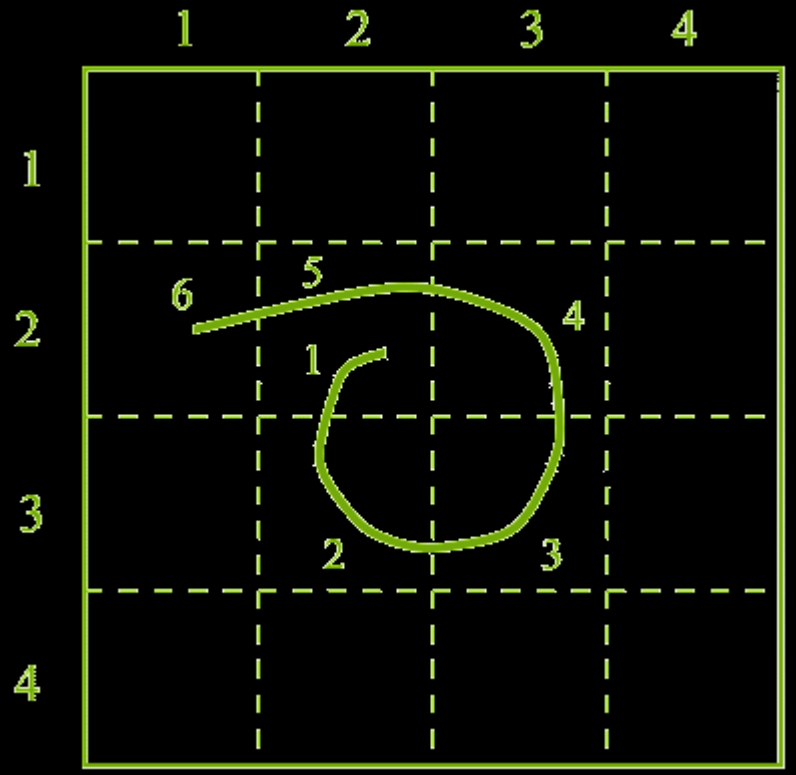
- Graphical passwords are knowledge-based authentication mechanism which leverage human memory for visual information with the shared secret related to or composed of images or sketches to improve the memorability of passwords while reserving the security of traditional passwords.
- Types:
  - Recall-based
  - Recognition-based
  - Cued-recall

Graphical passwords: Learning from the first twelve years - Biddle, Chiasson, et al. - 2011

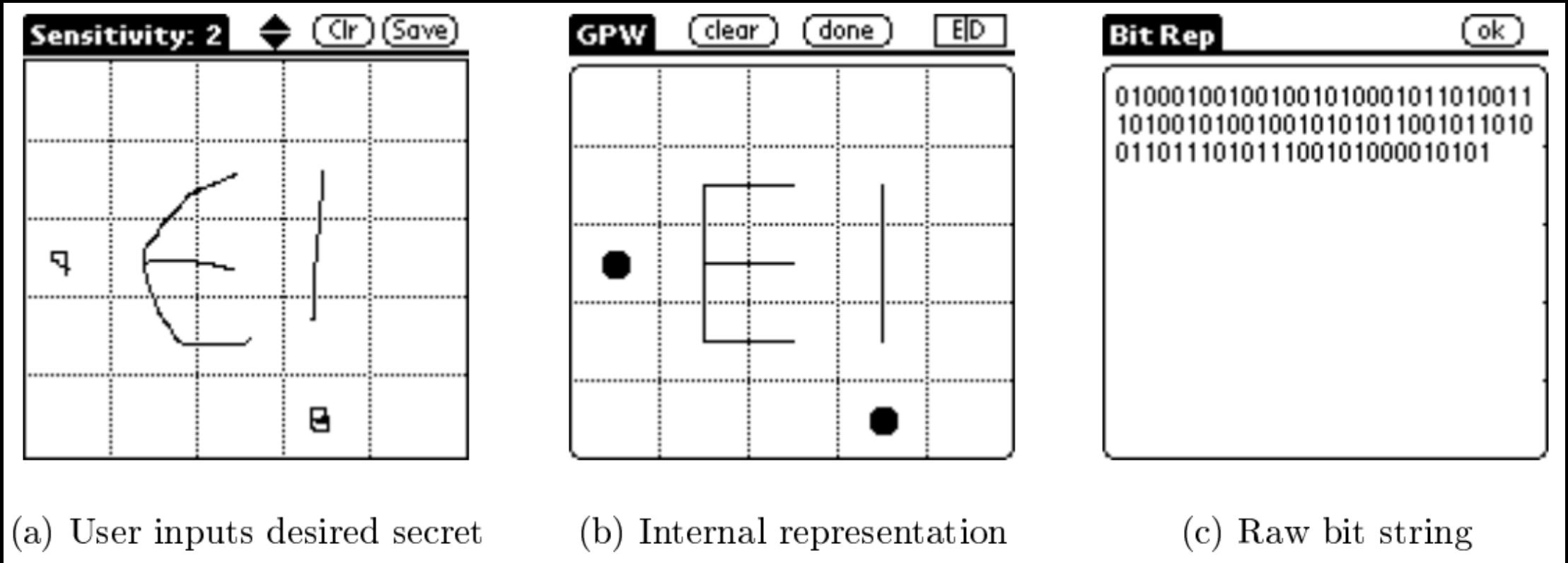
Recall-based system

- Draw & Recall
- Examples
  - Draw-A-Secret (DAS)
  - Pass-Go

Draw-A-Secret (DAS)

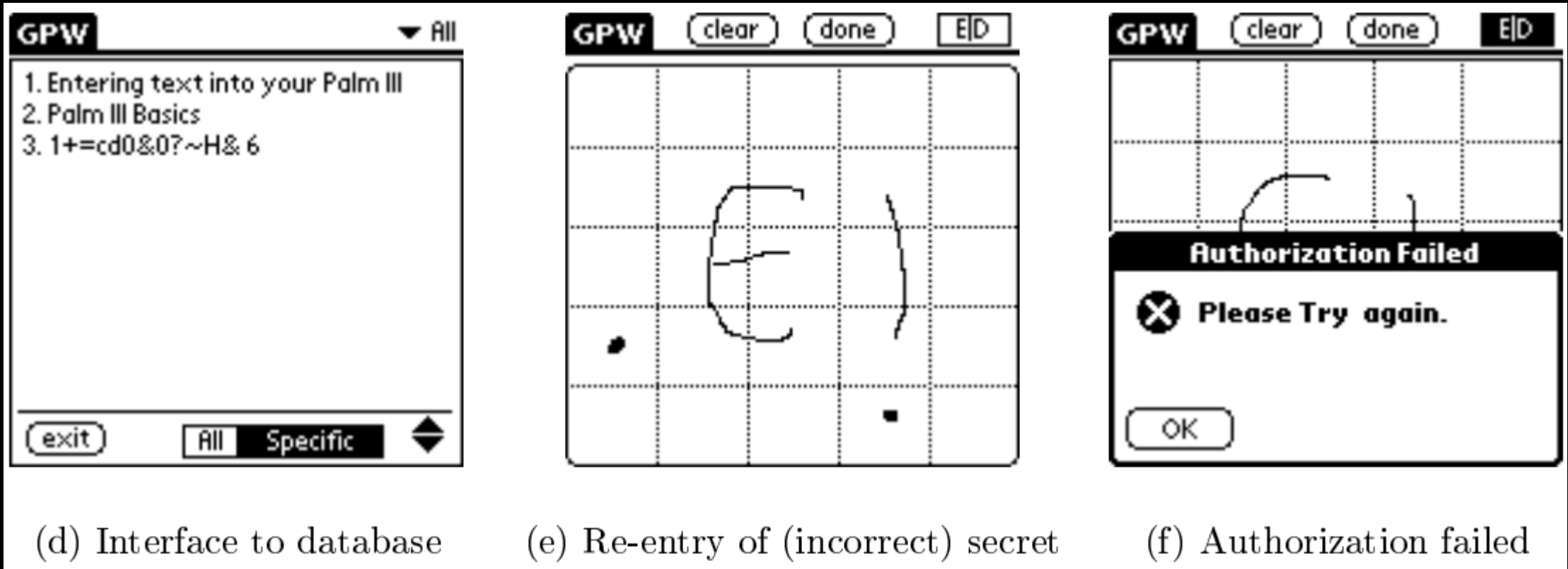


Draw-A-Secret (DAS)



(a) User inputs desired secret (b) Internal representation (c) Raw bit string

Draw-A-Secret (DAS)



(d) Interface to database (e) Re-entry of (incorrect) secret (f) Authorization failed

Recognition-based System

- Password Creation
  - Memorize a portfolio of images in password creation
- Login
  - Recognize those chosen images among decoys to log in
- Examples:
  - Passfaces
  - Story

Passfaces

- Password Creation
  - Users pre-select a set of human faces.
- Login
  - users select the face belonging to their choices among decoys in a panel of candidate faces.
  - The process will repeat several rounds with different panel.
  - Only when each round is executed correctly will users login.

Password Manager

Password Manager

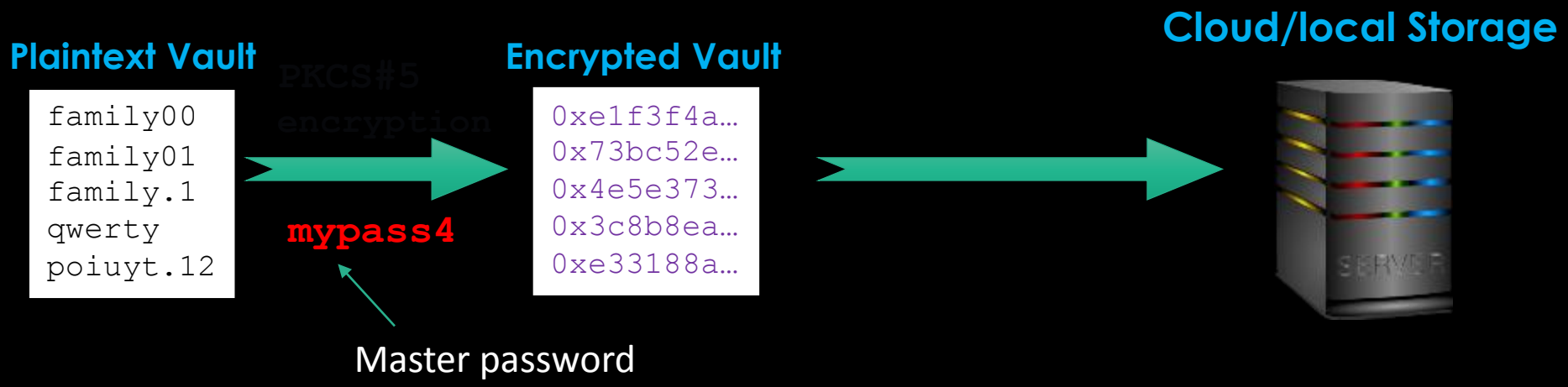
- Password manager is a software application or a hardware tool that can help users store and organize passwords.
- Motivation
  - Strong passwords are always complex
  - Too many account’s passwords to keep in mind
  - Password reuse leads to vulnerability of password leakage

PwdHash

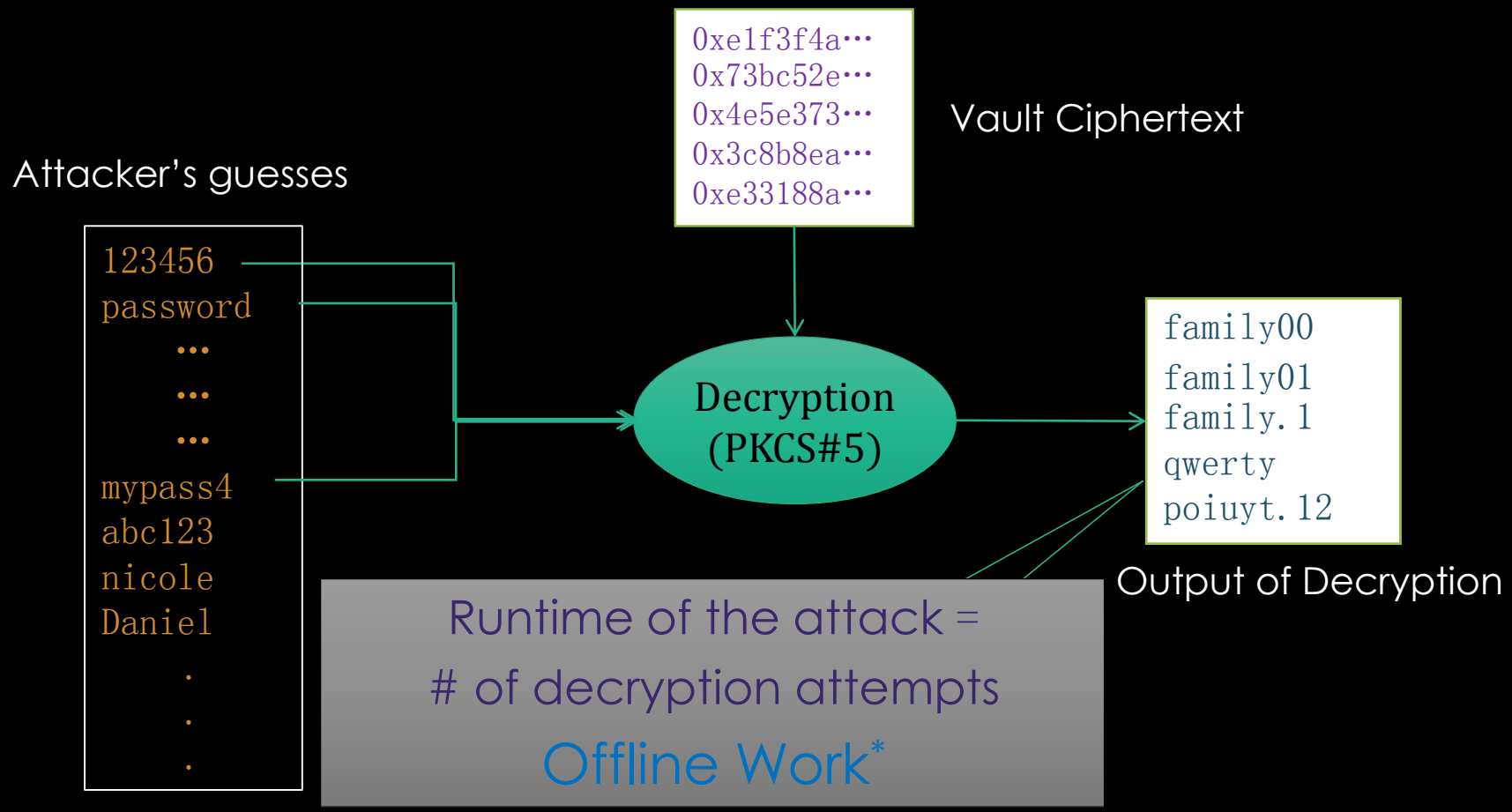
- Offered a solution

$$PWD(domain) = hash(mpw, domain)$$

Password Vault



Offline Attacks



LastPass e.t.c

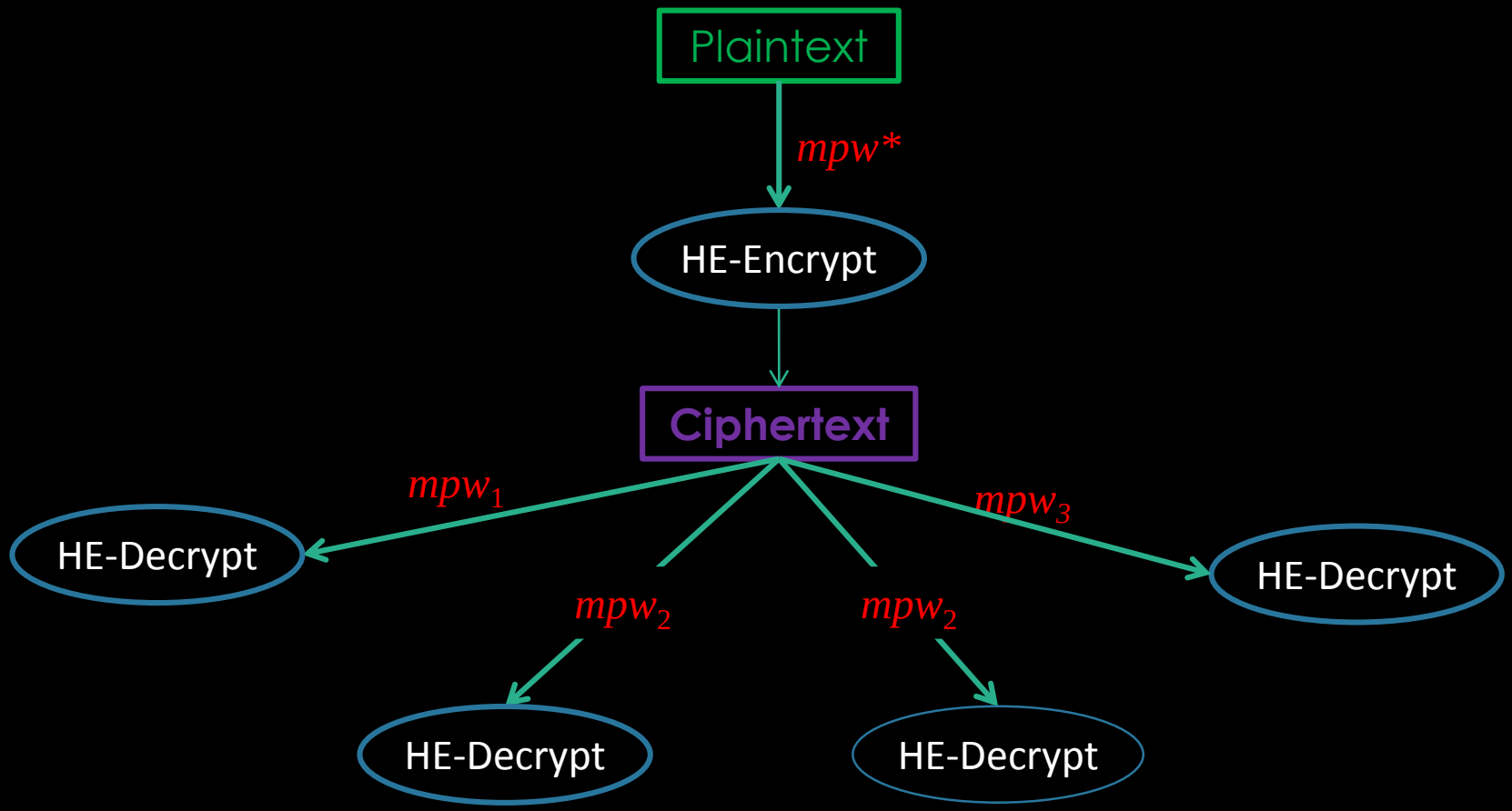
- Commercial Password Managers
- Storing user passwords on secure servers with
  - AES-256 encryption
  - 10000+ PBKDF2 iterations
  - No information of master password stored
- Vulnerabilities
  - Phishing attacks
  - Server attacks
  - Weak master passwords

Kamouflage

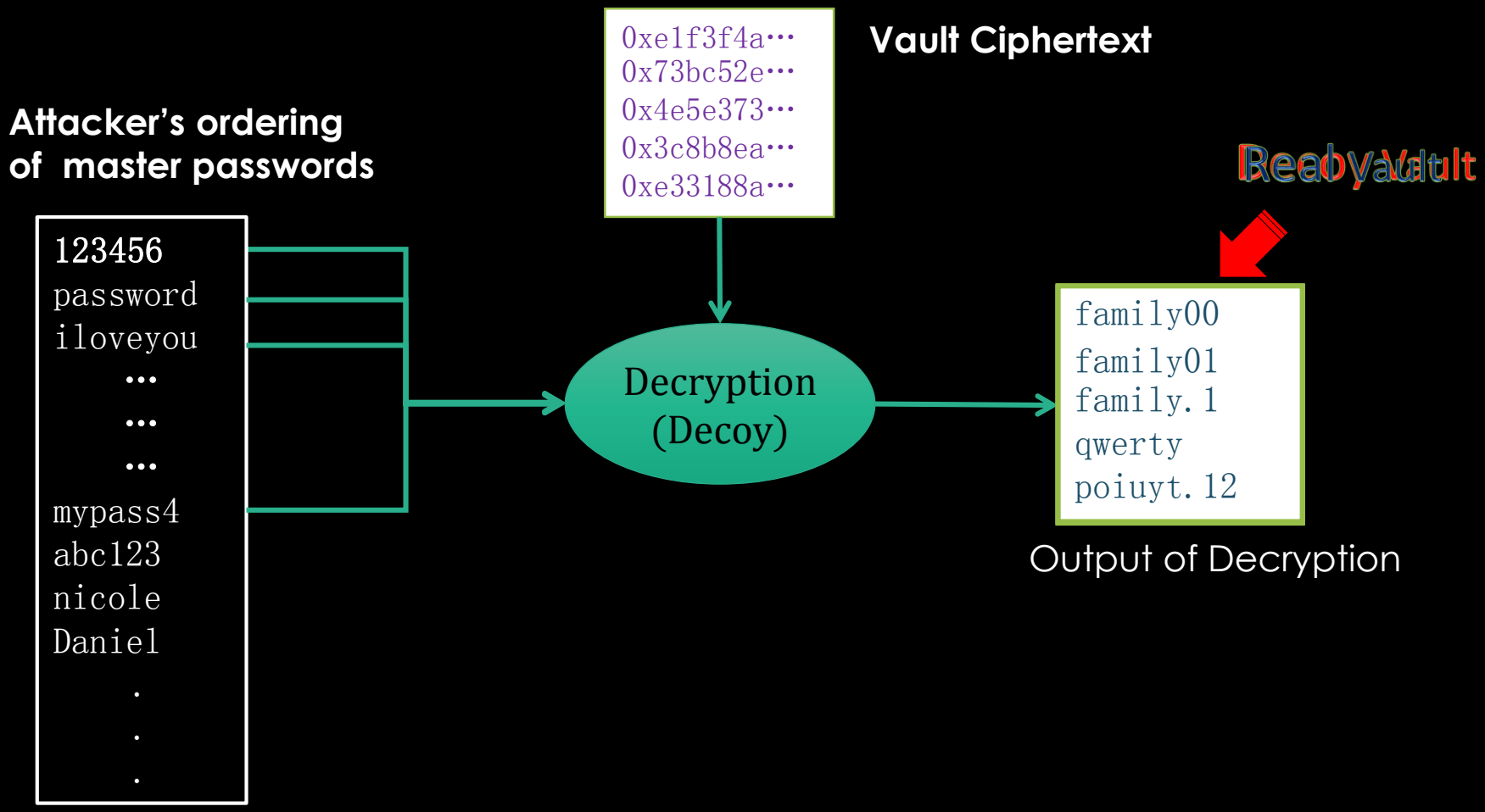
- Motivation
  - Weak master passwords are vulnerable to guessing attacks
- A clever idea
  - Add decoy master passwords and decoy password files
  - Store encryption of a true vault with N-1 decoy vaults encrypted under decoy master passwords

Hristo Bojinov, Elie Bursztein, Xavier Boyen, Dan Boneh . Kamouflage: Loss-Resistant Password Management, ESORICS 2010.

Honey Encryption



Honey Encryption

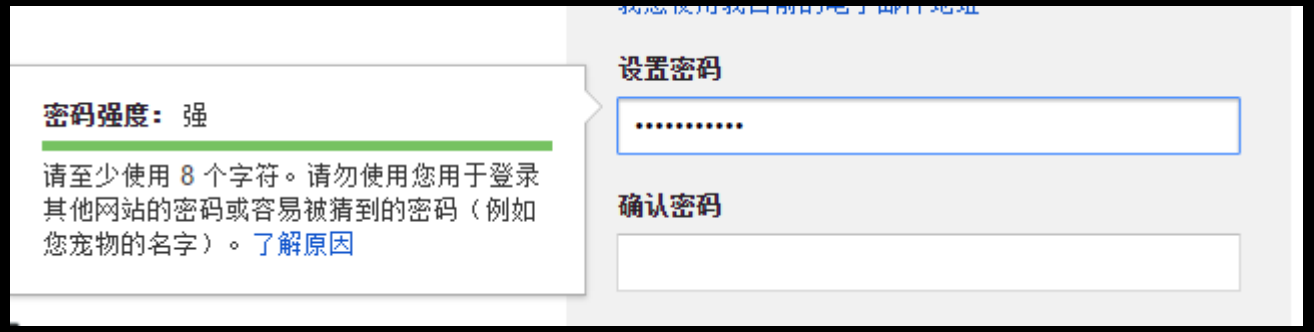


Password Meter

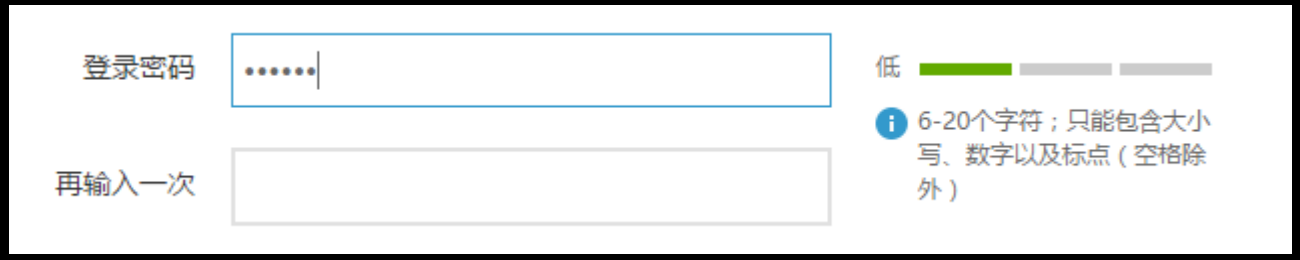
Password Meter

- Used to measure password strength

Google



CSDN



Password Meter——Password Strength

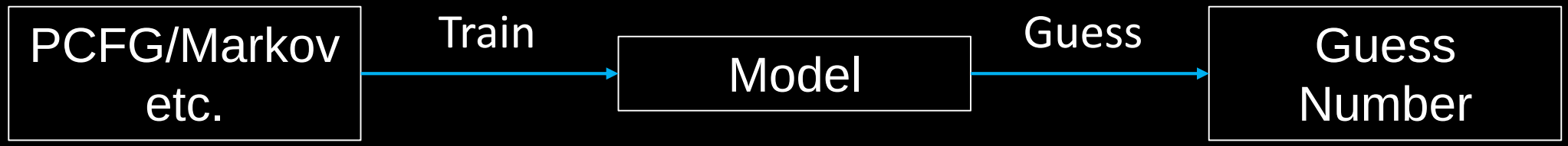
- National Institute of Standard and Technology (NIST): SP800-63

  - The entropy of the first character is 4 bits
  - The entropy of the next 7 characters is 2 bits per character
  - for the 9th through the 20th character the entropy is taken to be 1.5 bits per character
  - for characters 21 and above the entropy is taken to be 1 bit per character
  - Bonus: Uppercase Letters, Special Characters, not in dictionary

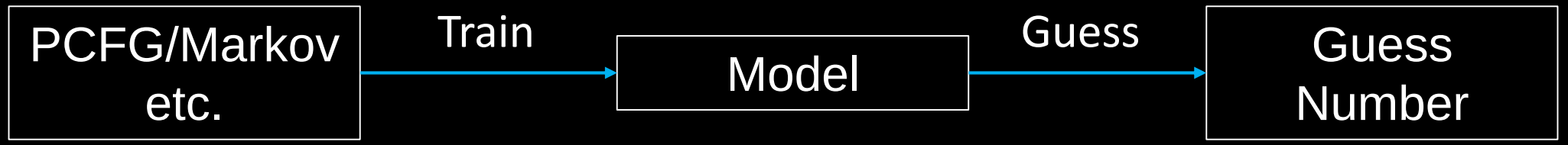
Password Meter——Password Strength

- password
- 123456
- nihao
- woshiyizhiyu
- 4Ve$(n

Password Meter——Guess Number



Password Meter——Guess Number



Guess Number Calculator: Kelly *et al.*

——*Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms.*

Password Meter——Defect of PCFG/Markov

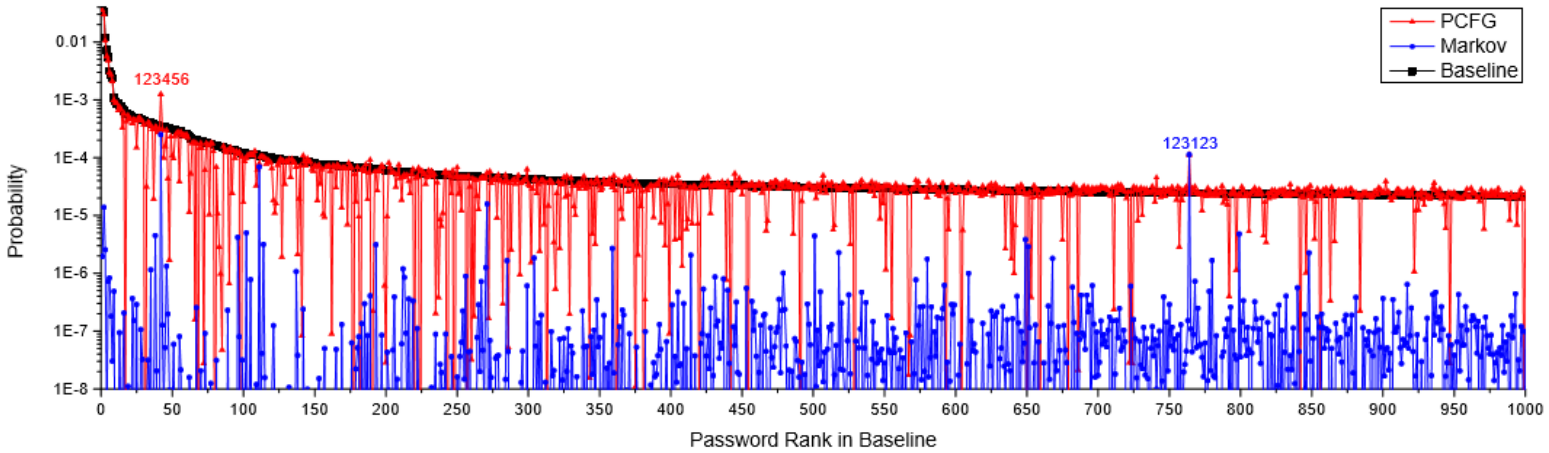


Fig. 1. The baseline probabilities of the most popular 1000 passwords in CSDN and the ones predicted by PCFG and Markov Methods.

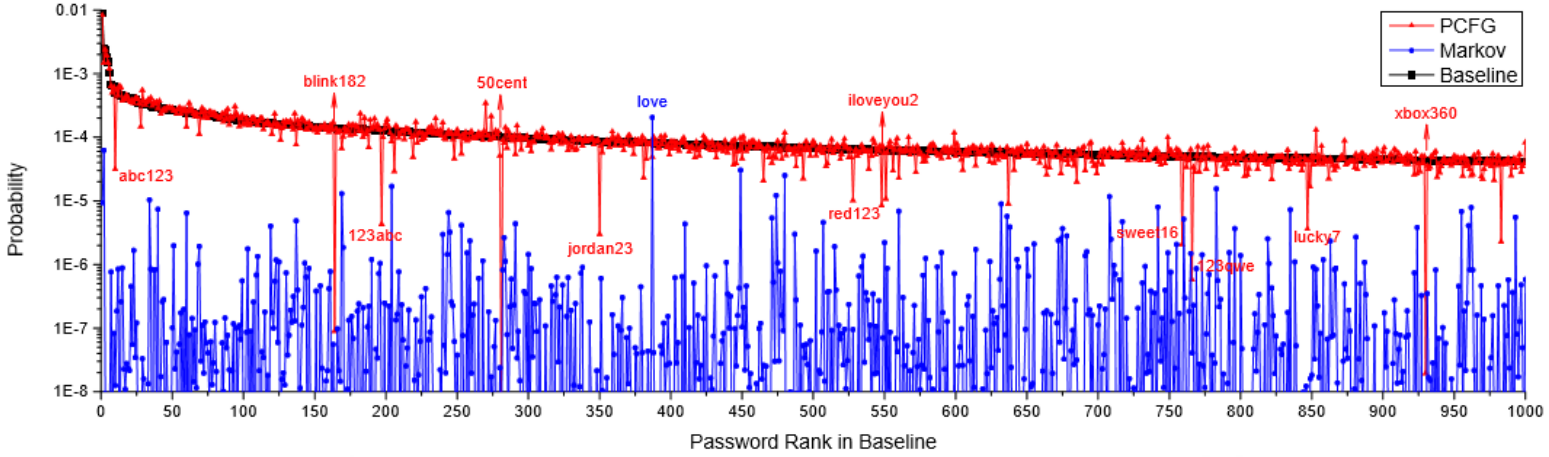


Fig. 2. The baseline probabilities of the most popular 1000 passwords in Rockyou and the ones predicted by PCFG and Markov Methods.

Properties of Chinese Passwords

Properties of Chinese Passwords

[1] Zhigong Li, Weili Han, Wenyuan Xu. *A Large-Scale Empirical Analysis of Chinese Web Passwords[A].* In 23rd USENIX Security Symposium (USENIX Security 14), 2014: 559–574.

[2] Weili Han, Zhigong Li, Lang Yuan, Wenyuan Xu. *Regional Patterns and Vulnerability Analysis of Chinese Web Passwords[J].* IEEE Transactions on Information Forensics and Security, 2016, 11(2): 258–272.

[3] Weili Han, Zhigong Li, Minyue Ni, Guofei Gu and Wenyuan Xu. *Shadow Attack based on Password Reuses: A Quantitative Empirical View[J].* IEEE Transactions on Dependable and Secure Computing, 2016 (minor revision)

Properties of Chinese Passwords

Over 100 million clear-text passwords

If you want to guess his/her passwords:

50% Digit-only Password

If you want to guess his/her passwords:

10% Letter-only Password

If you want to guess his/her passwords:

35% Letter+Digit Password

If you want to guess his/her passwords:

3.5% is “123456”

If you want to guess his/her passwords:

1% is “111111”

If he/she uses letters:

30% is Pinyin

If he/she uses pinyin:

1.5% is “woaini”

Using our findings

We improve the guessing efficiency of PCFG-based method by **34%**

Password Reuse

34% reuse their passwords

When they do not reuse passwords

When they do not reuse passwords

We improve the dictionary guessing efficiency of John the Ripper by **39%**

Call for Participants (http://www.sacmat.org/)

We are organizing SACMAT 2016, the top conference in the field of Access Control. Welcome to register and attend.

Q&A