Multi-armed bandit approach to password guessing

Hazel Murray & David Malone
Maynooth university, Ireland

Who Are You?! Adventures in Authentication Workshop (WAY) 7th August 2020

Contents

Motivation

Facebook 13
Facebooku
computerispowerfacebook

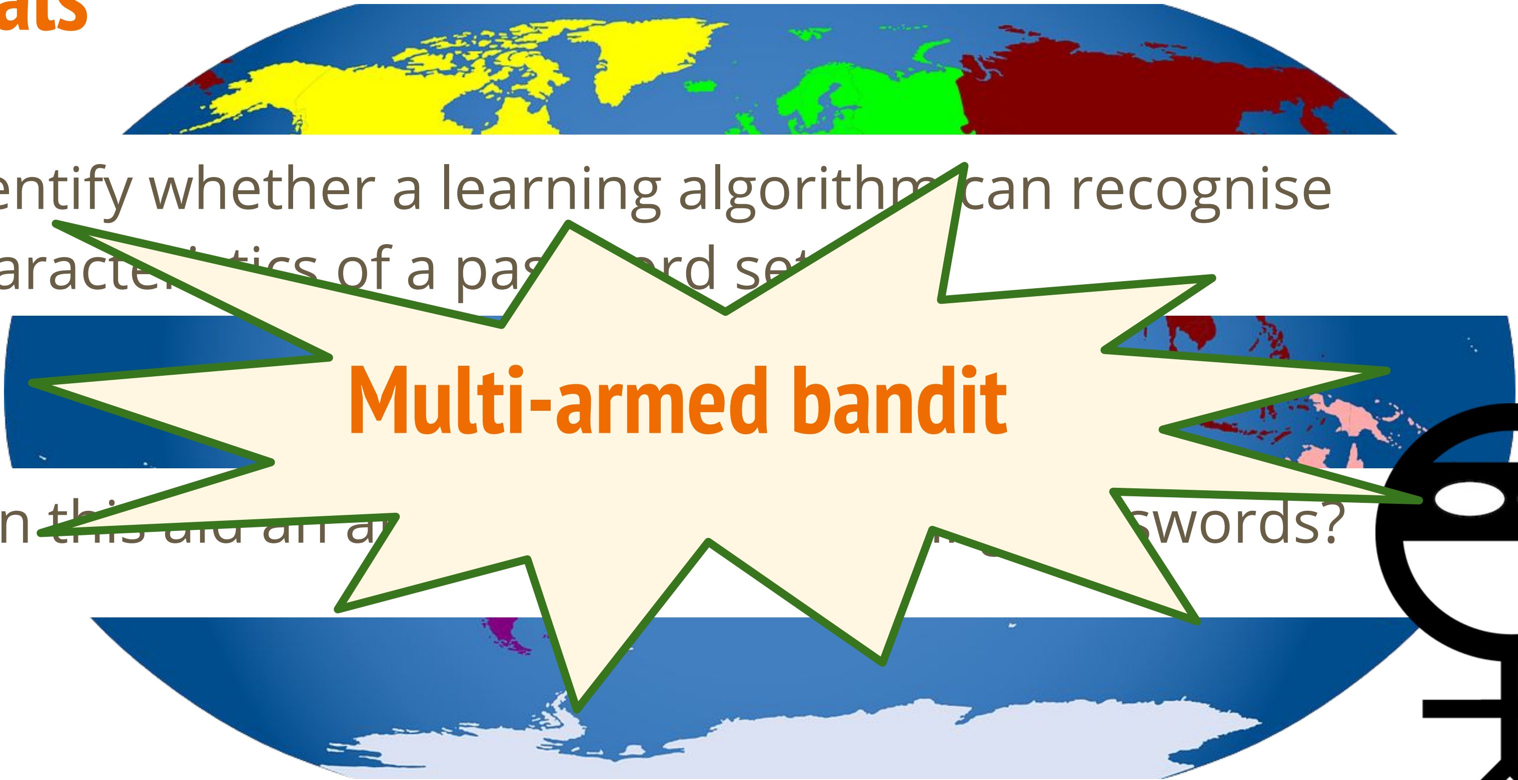
linkedin
LinkedIn
jobsearch

Wei, M., Golla, M. and Ur, B., 2018. The Password Doesn't Fall Far: How Service Influences Password Choice. *Who Are You.*

Motivation

- Ibare, J., Musungu, J. and Kigali, R., A comparison of common passwords in East Africa against common passwords in the United States.
- AlSabah, M., Oligeri, G. and Riley, R., 2018. Your culture is in your password: An analysis of a demographically-diverse password dataset. *Computers & security*, *77*, pp.427-441.

Goals



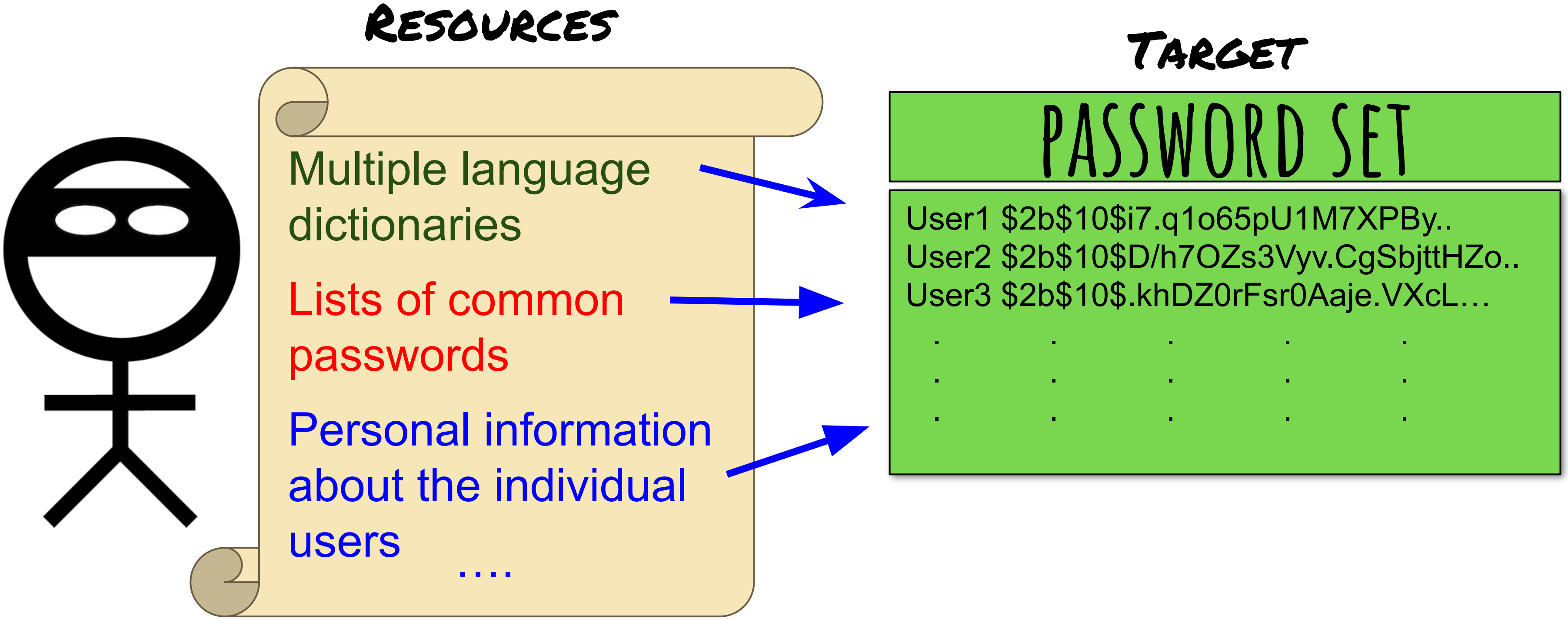
Identify whether a learning algorithm can recognise characteristics of a password set

Multi-armed bandit

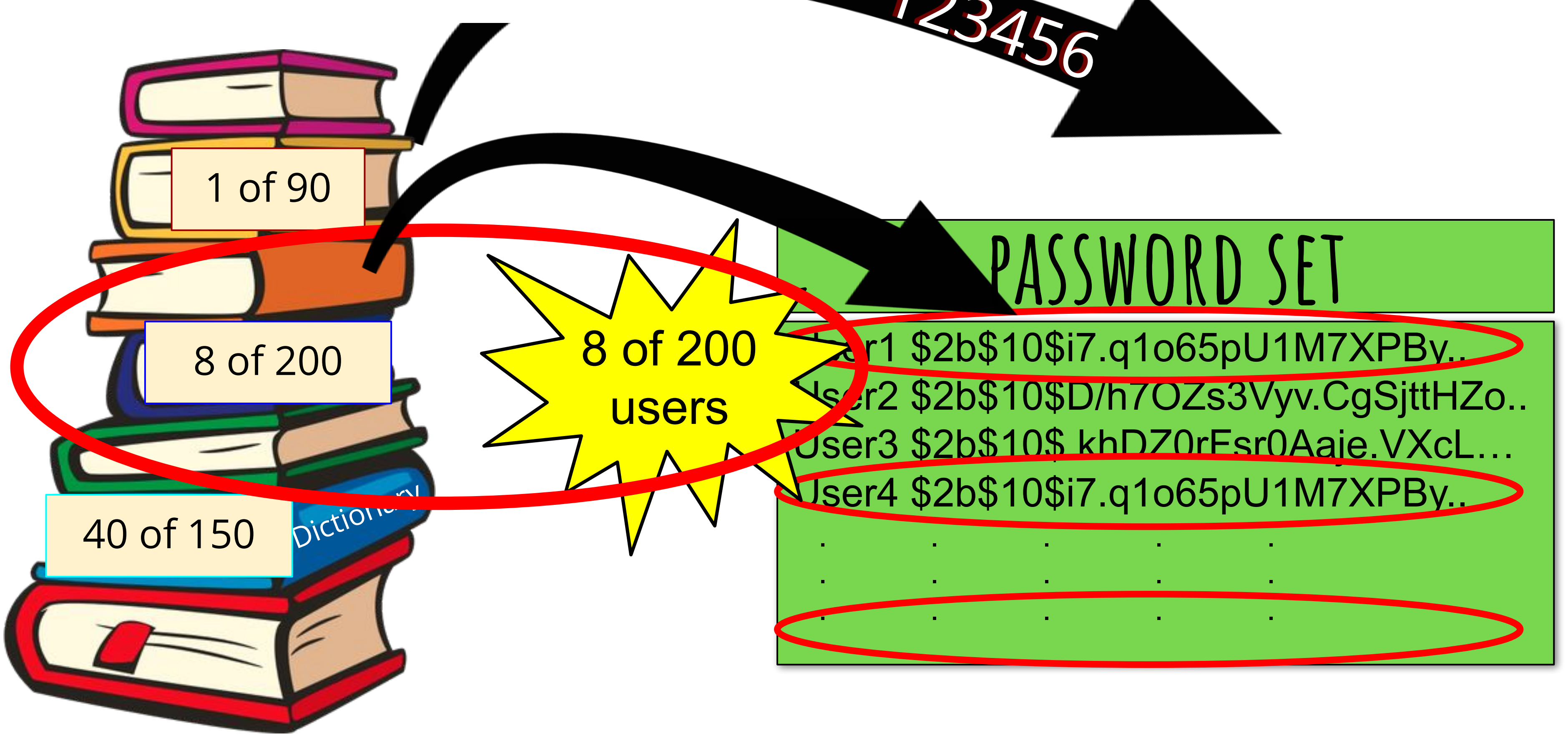
Can this aid an a … swords?

Multi-armed bandit

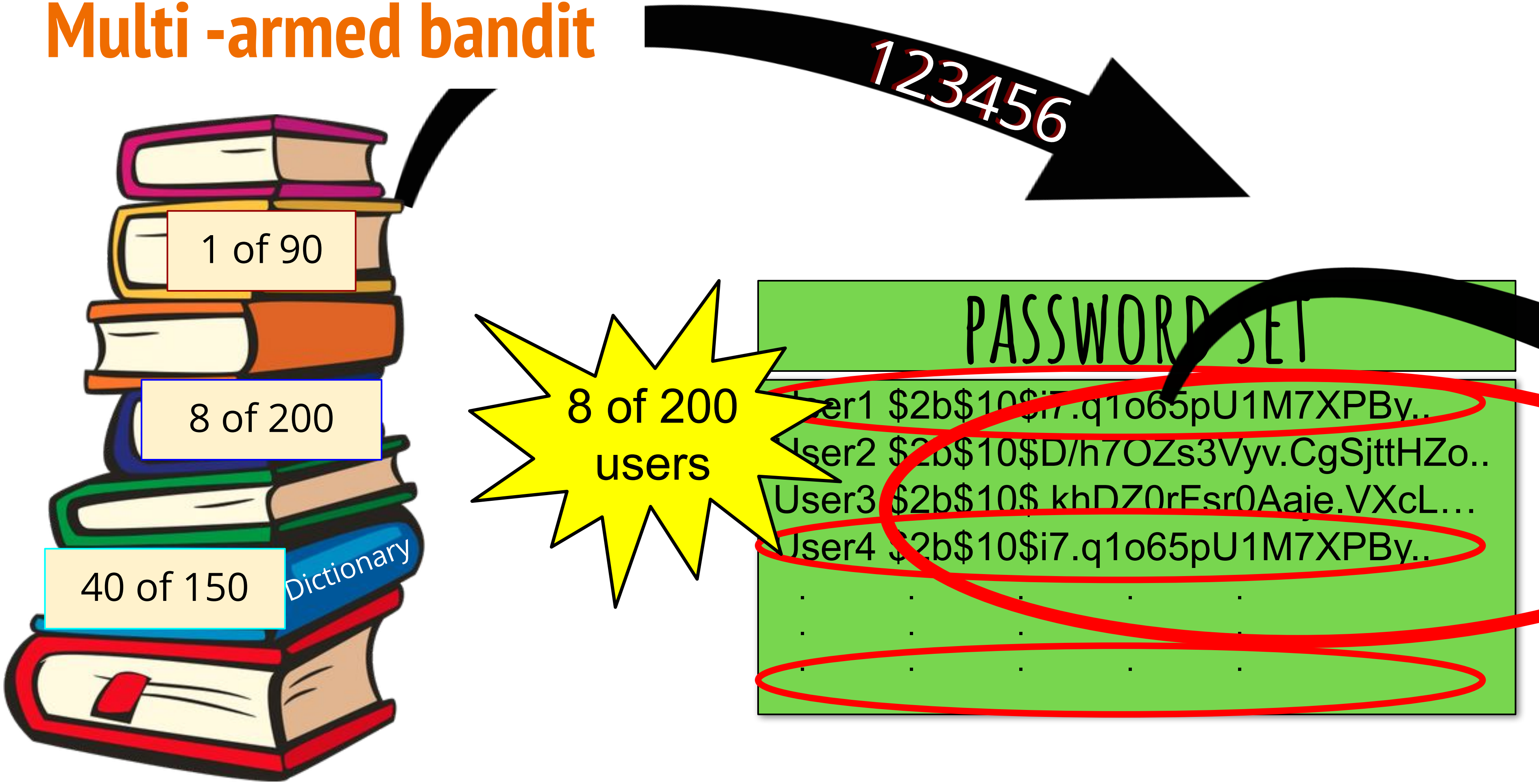
A multi-armed bandit password attacker



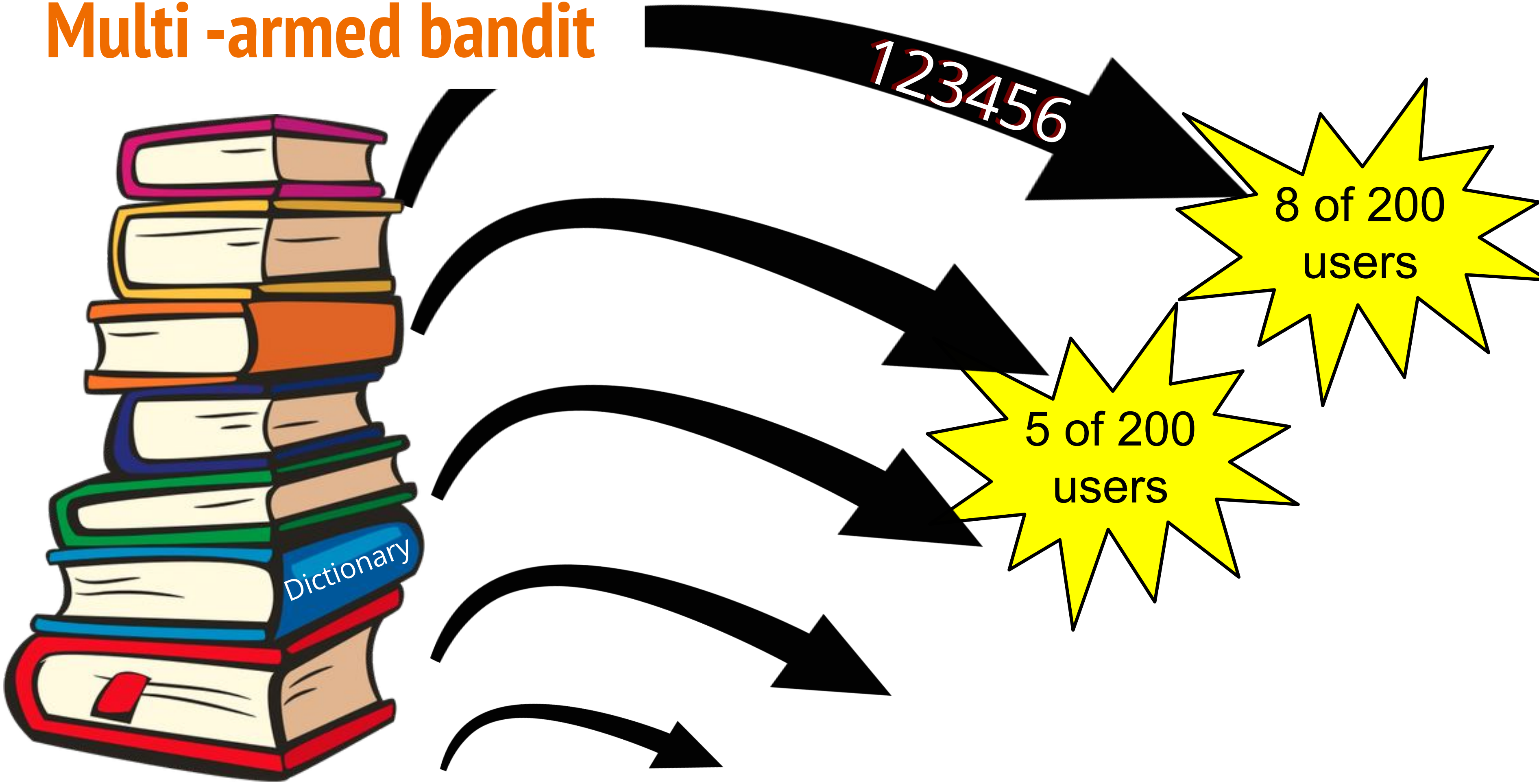
Multi -armed bandit



Multi -armed bandit



Multi -armed bandit



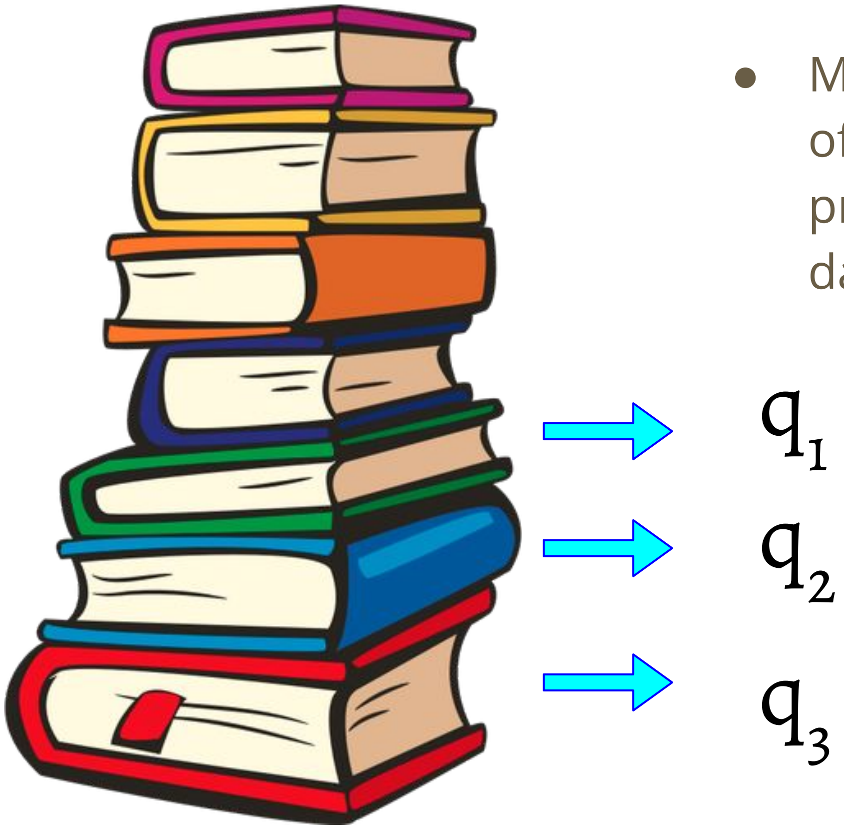
Learning Techniques

There are two learning techniques we are employing here:

- Matching the proportions seen to those in the dictionaries we have
- Making informed guesses based on this information.

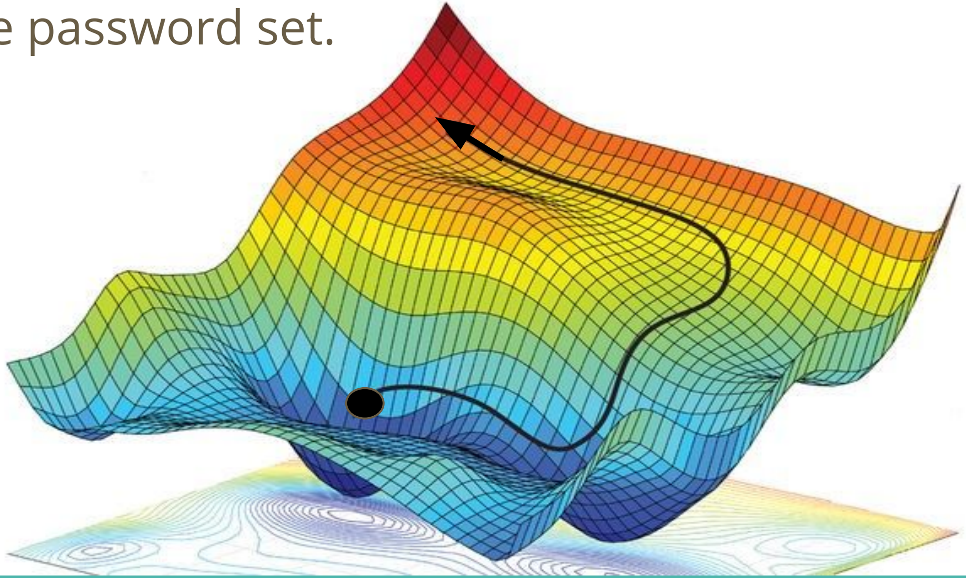
Maximum likelihood

- Maximum likelihood estimation is a method of estimating the parameters of a probability distribution using observed data.



Maximum likelihood

- Except in limited cases, the likelihood cannot be solved explicitly to find the maximum.
- We used a technique called gradient descent to converge towards the q values that best describe the password set.



Informing our guesses

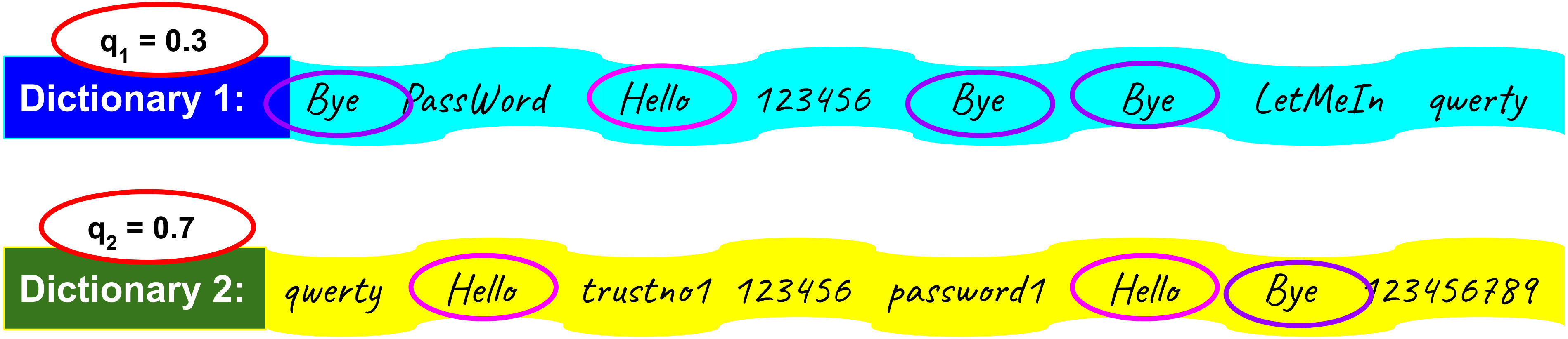
We have three ways of choosing our guesses:

1. Randomly choose a dictionary to guess from and choose the next most probable word from that dictionary. (exploring)

2. Choose the next best password from the dictionary which seems to be the best match for the password set we are guessing (exploiting)

3. Choose guesses based on information about the frequency of words and the weightings of all the dictionaries we have: Q method

Q method



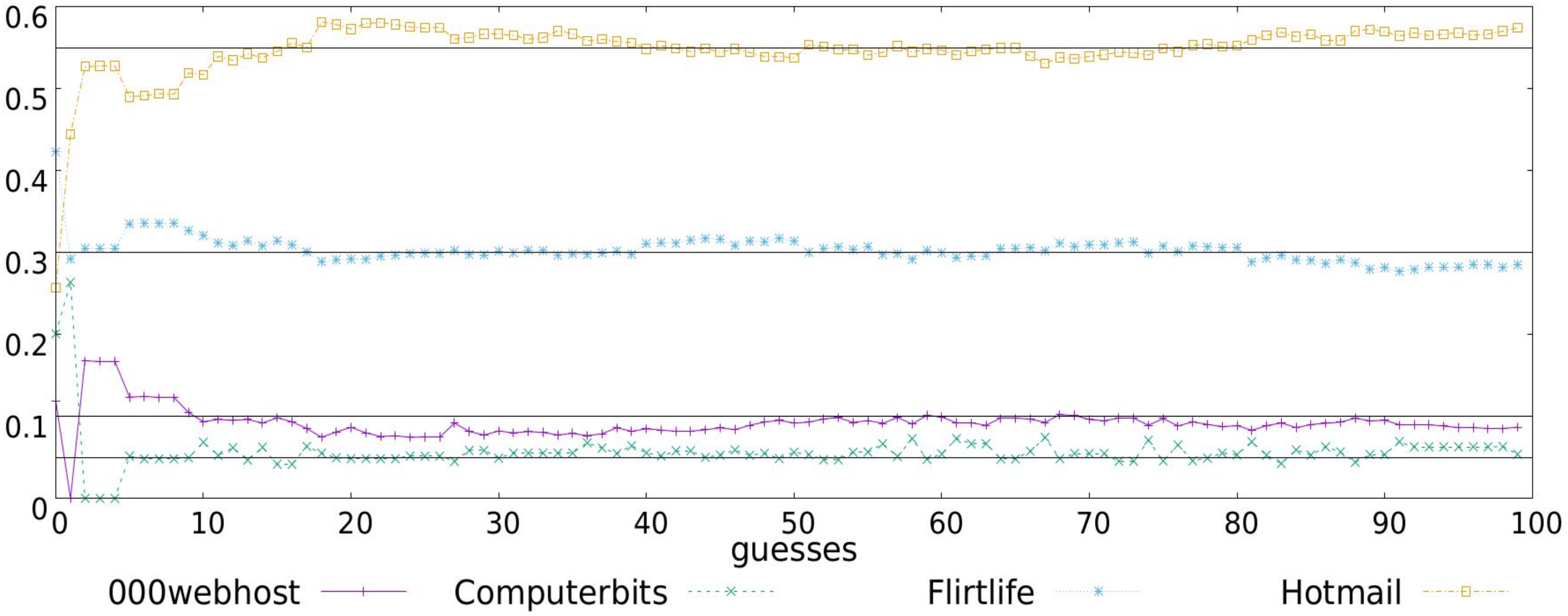
$$Q(\text{“Hello”}) = (1/8)(0.3) + (2/8)(0.7) = 0.2125$$

Multi-armed Bandit Results.

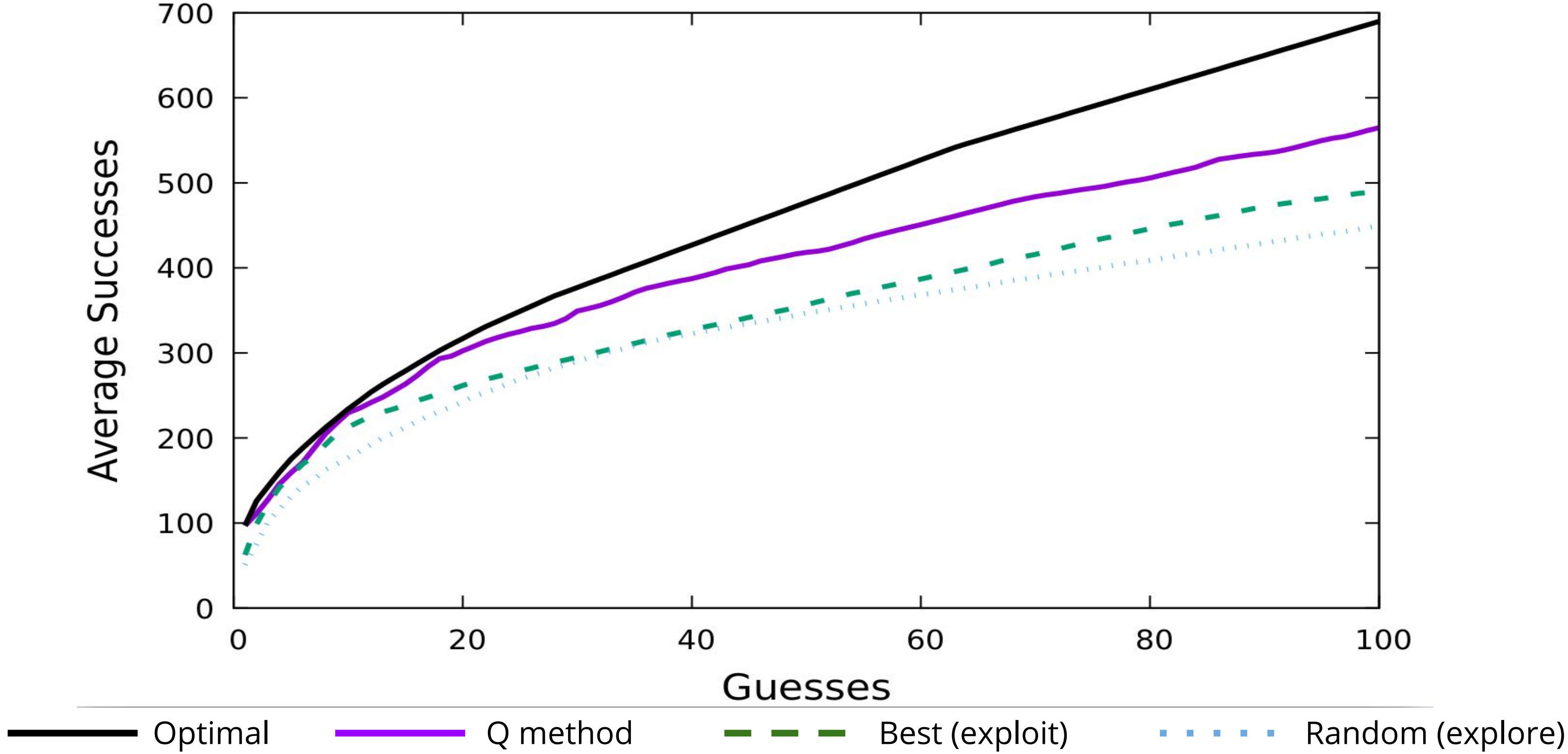
We created a simulated password set which is a sample of 10,000 users where

- 5500 came from hotmail.com
- 3000 came from flirtlife.de
- 1000 came from 000webhost.com
- 500 came from computerbits.ie

Estimation of dictionary weightings



Guessing success



Impact

- Guessing improvement - particularly relevant to online attackers who could use the learning in **automated guessing**.

- Discourage **Users** from choosing passwords related to the website name or type.

- Because we can automate the recognition of these patterns, this could be used to inform **password strength meters and blocklists**.

Hazel Murray hazel.murray@mu.ie
David Malone David.malone@mu.ie
Maynooth University, Ireland

Informing our guesses

The multi armed bandit is based on the principle of exploring and exploiting. In that sense we want to learn about all the different dictionaries we have while exploiting the most closely matching dictionary.

One advantage of our multi-armed bandit set up is that when we make a guess we learn something about all the dictionaries because the password we guess will occur with some proportion in all the dictionaries. That portion could be zero and we have still learnt something.

Testing maximum likelihood