CPSC 530 PRESENTATION

STRENGTH AND PREDICTABILITY OF GRAPHICAL PASSWORDS

Alex Tanasescu - Computer Science - 30041538
Matthew Newton - Computer Science - 30094756
Delara Shamanian Esfahani - Computer Science - 30089408
Ramez Halasah - Computer Science - 30094242

GROUP 4

Overview + Content

- Three Questions
- Types of Graphical Passwords
  - Android 3x3 Password
  - Colour Based 3x3 Password
  - Picture Based Password
- Analysis
  - Heatmaps
  - Entropy Estimation
  - Trends

Three Questions

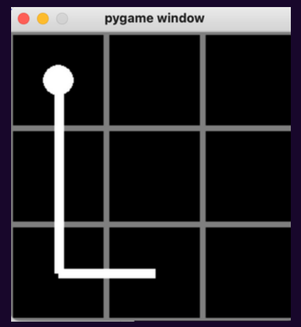
1. For the picture password, where a user would choose a point from 4 pictures in order, would the theoretical entropy match the experimental entropy?
2. Name a test that is appropriate for measuring/estimating entropy of a password
3. Given the 3x3 coloured graphical password, was there a colour that reduced the strength of the password? Explain your reasoning.

Types of Graphical Passwords

01

Android 3x3 Password

Standard Android pattern password style



02

Colour Based 3x3 Password

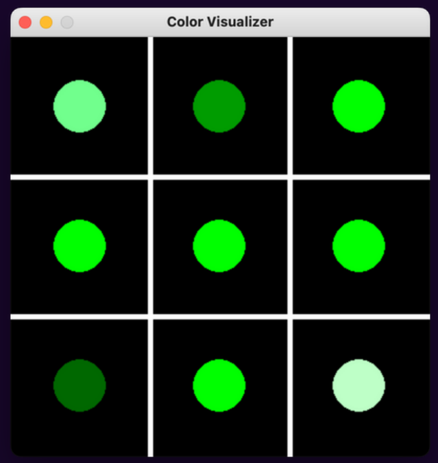
Users will choose their password based on the colours given in a 3x3 grid.

03

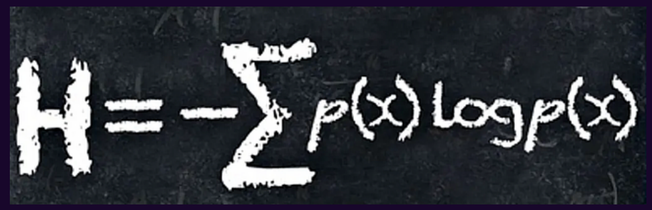
Picture Based Password

Users choose their password based on clicking on points in a picture

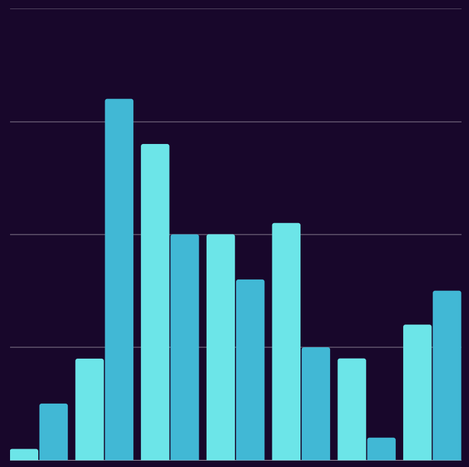
Analysis



Heatmap

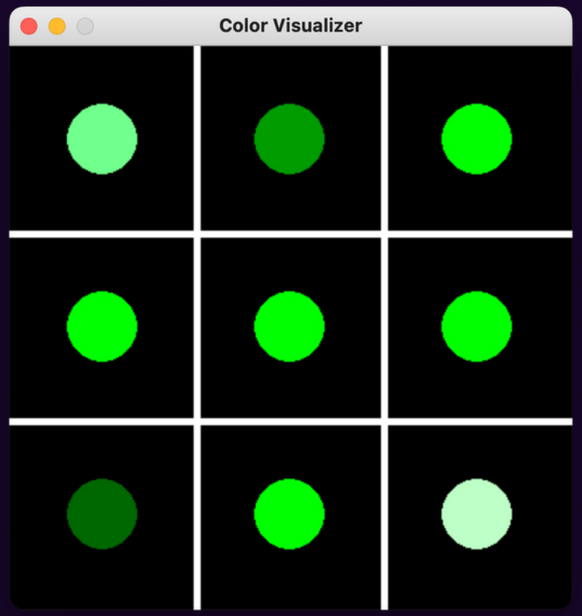


Entropy Estimation



Trends

Heatmaps

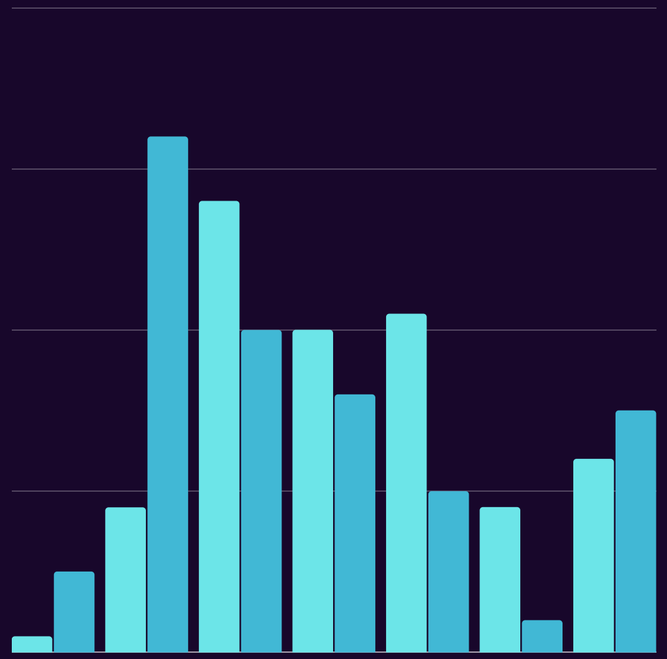


- Overlayed each password dataset to generate heatmaps
- Heatmaps show the frequency that each cell is chosen
- Darker colour indicates higher frequency of clicks

Entropy

- Calculate max entropy assuming uniform distribution
- Compare result with our generated distribution

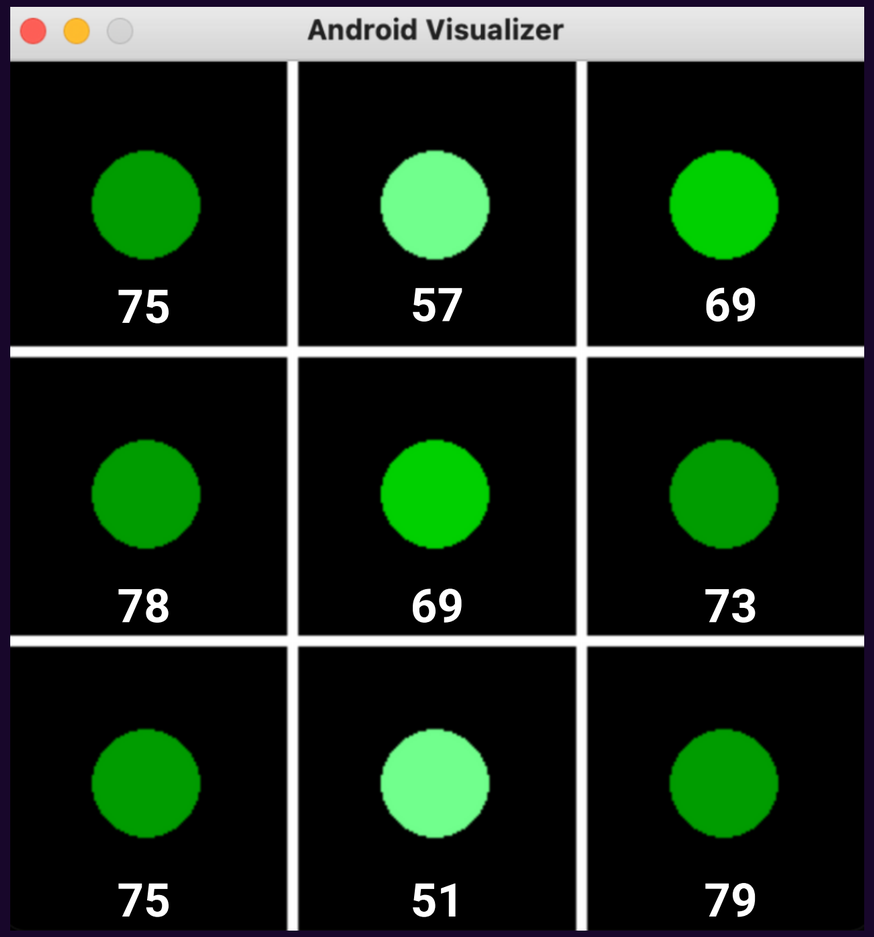
Trends



- Compared passwords by looking for patterns
- Examples: length, common element in a password

Android Password

- Most passwords tended to heavily use the corners
- Cell 2 and Cell 8 were chosen the least
- Not a lot of variation between those clicked frequently and those clicked not that frequently
- Even though our sample size is small. Our findings reflect common findings others have found in a larger sample size[2]

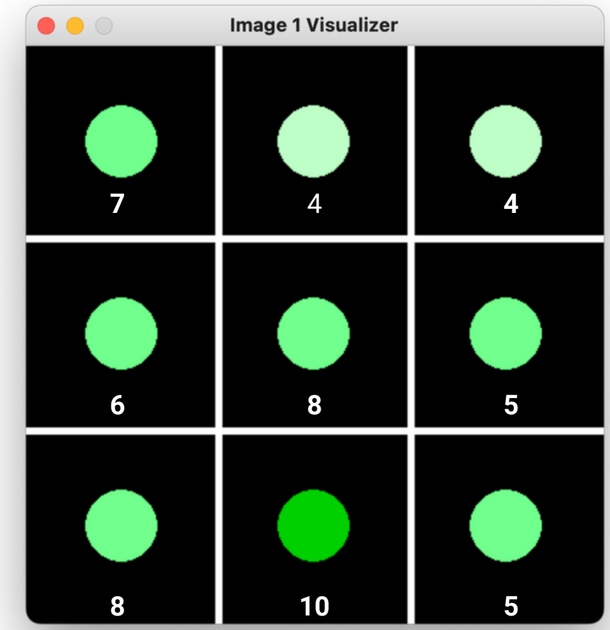


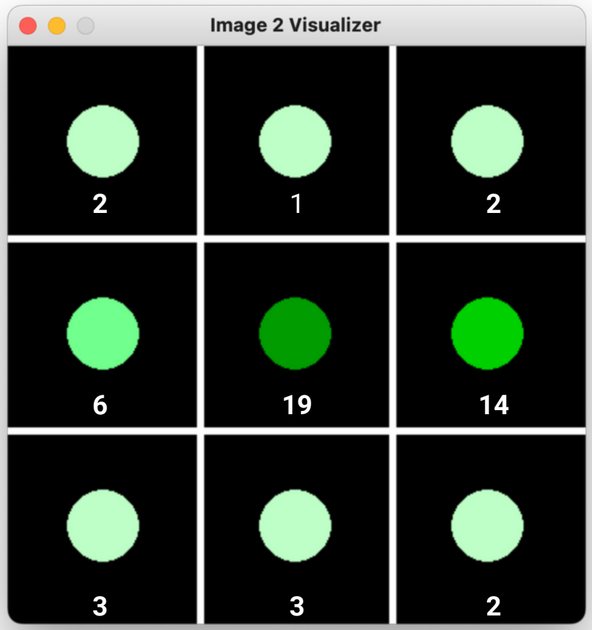
Colored Password

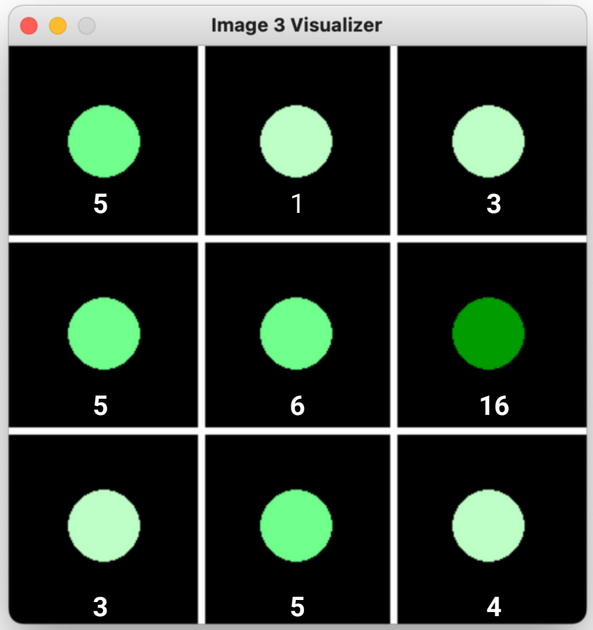
- Cells represent the colours that have been clicked
- Way more variation than android password due to less restrictions
- If a colour was frequently clicked (such as red), this reduces the entropy of system and therefore decreases the strength of the passwords

HEATMAPS

Picture Password

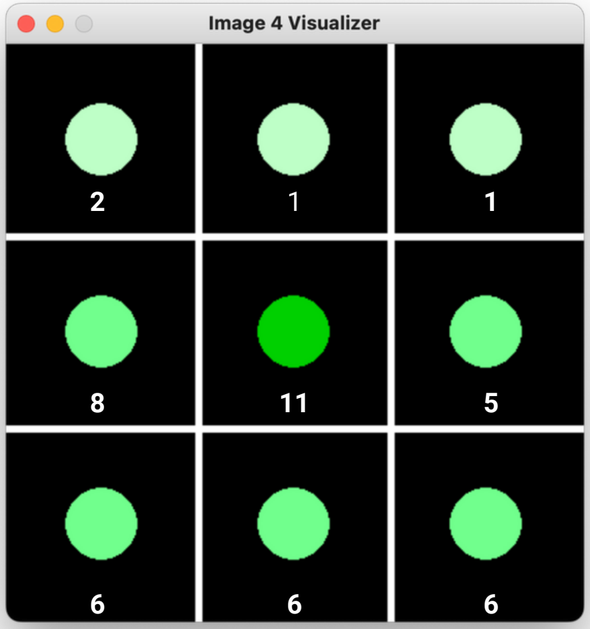


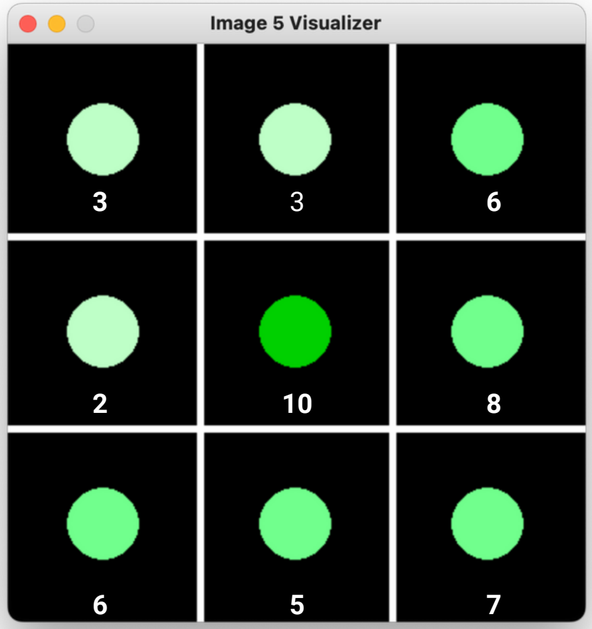


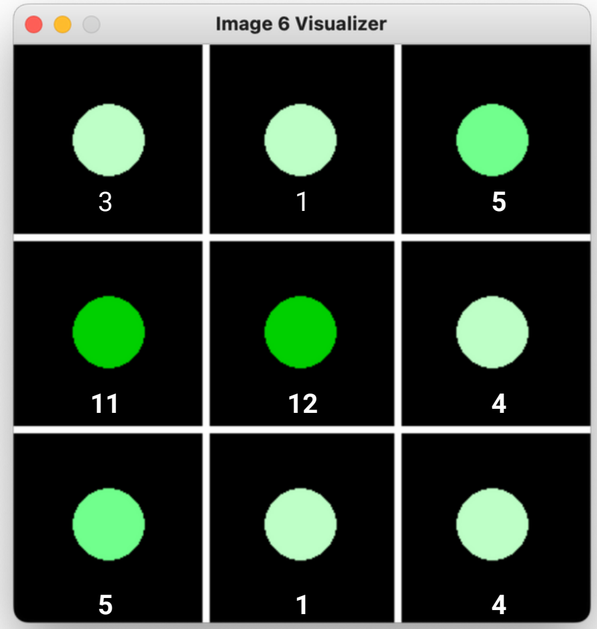


HEATMAPS

Picture Password Cont.

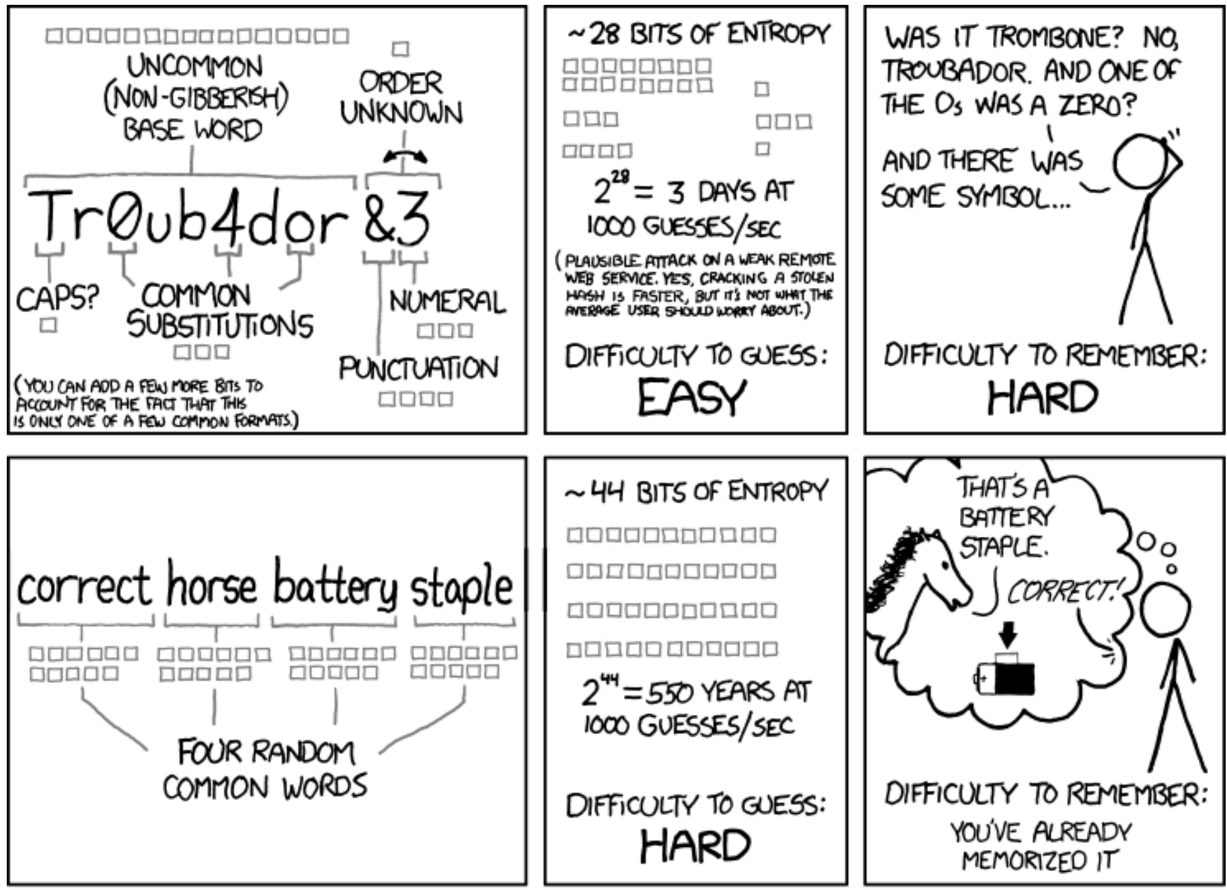






Entropy

- Entropy can be used as a way to determine the theoretical strength of a password assuming the password type has a uniform distribution.
- Based on number of possible combinations for each system
- Can be measured by entropy estimation using Shannon's entropy



Android Entropy

- Determine the number of possible combinations
- Using a combination generator we found with a minimum of 3 dots and max 9 the total possible combinations is 389436 [1]
- Uniform distribution for max entropy

$$\log_2(N) = \log_2(389\ 436)$$
$$= 18.571 \text{ bits}$$

Color Entropy

- The possible number of combinations:
  - Password length can be 1 - 9
  - 3x3 grid
  - no restrictions
- Uniform distribution for max entropy

$$9 + 9^2 + 9^3 + 9^4 + 9^5 + 9^6 + 9^7 + 9^8 + 9^9$$
$$= 435\ 848\ 049$$
$$\log_2(N) = \log_2(435\ 848\ 049)$$
$$= 24.\ 108 \text{ bits}$$

Picture Entropy

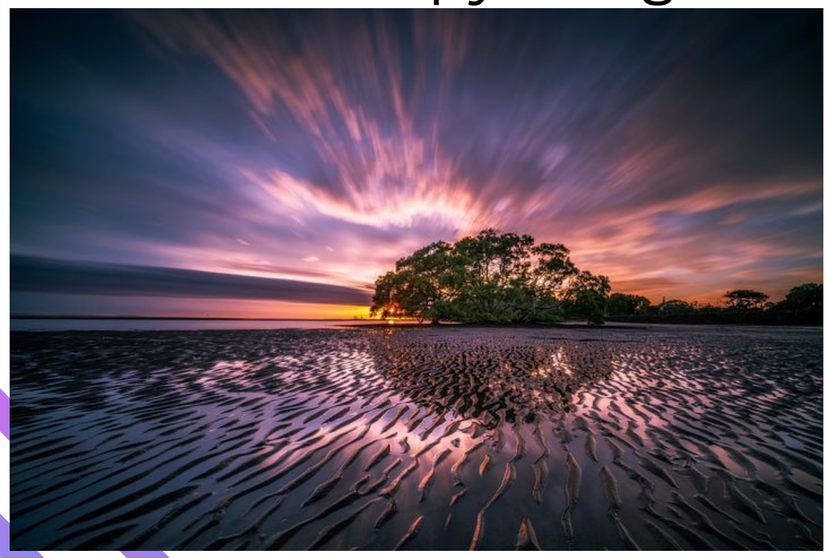
- Number of combinations:
  - Password consists of 3 pictures
  - Each picture split into 3x3 grid

$$9 \times 9 \times 9 = 729$$

$$\log_2(N) = \log_2(729) = 9.510 \text{ bits}$$

Best Entropy: Image 1

Worst Entropy: Image 2



Experimental vs Theoretical Entropy

Image 1 Experimental: 3.103 bits
Image 2 Experimental: 2.527 bits
Image 3 Experimental: 2.838 bits
Image 4 Experimental: 2.867 bits
Image 5 Experimental: 3.024 bits
Image 6 Experimental: 2.805 bits

ENTROPY

Theoretical Entropy vs Experimental Entropy for Picture Password System

Picture Password Entropy:

- Add entropy of 3 pictures to get total password entropy

Theoretical Uniform distribution (Max Entropy):

Max Entropy = 9.510 bits

Best Experimental Entropy (uses Image 1, 4, 5):

Best Experimental Entropy: 8.994 bits

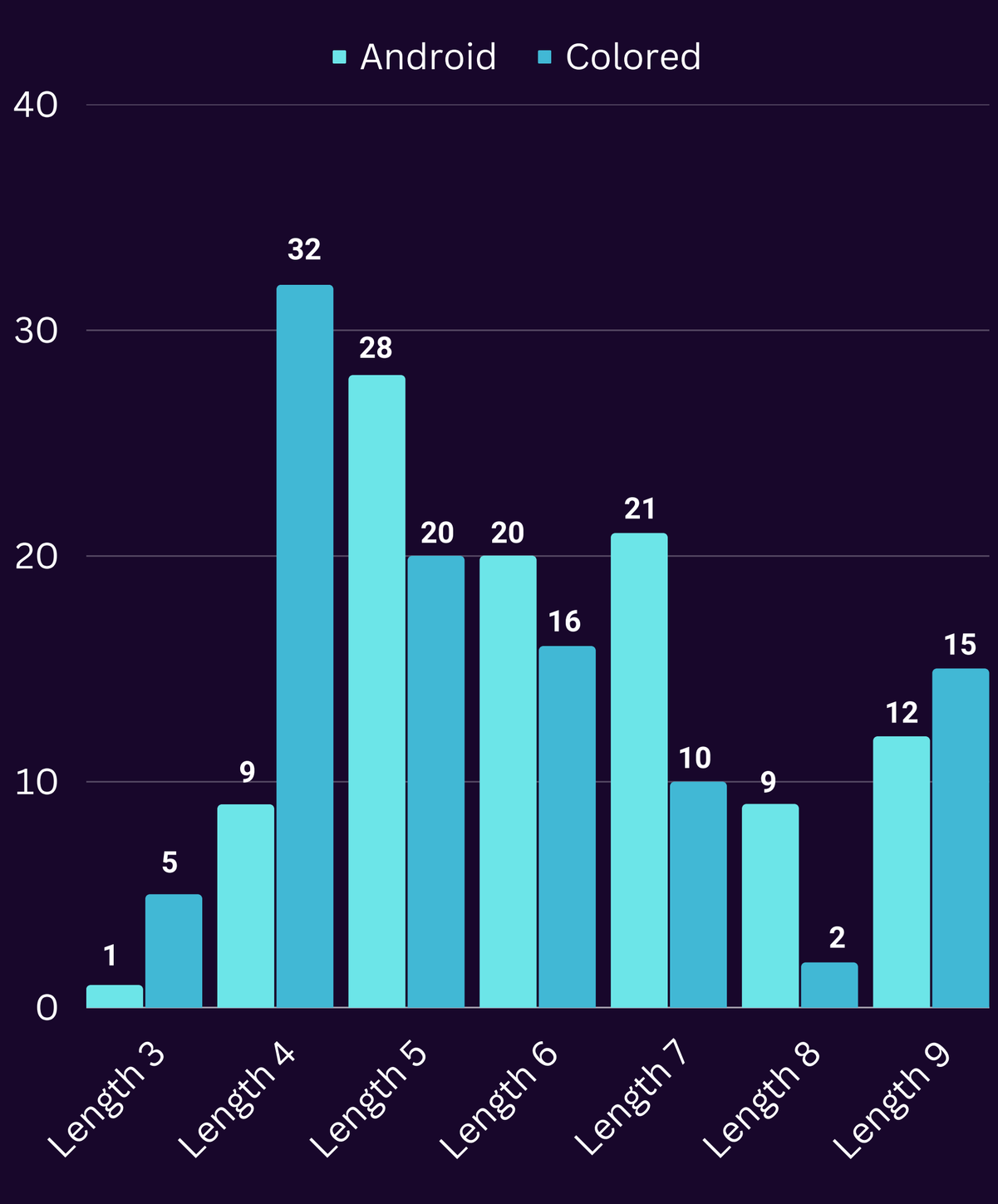
Worst Experimental Entropy (uses Image 2, 3, 6):

Worst Experimental Entropy: 8.170 bits

Why is our experimental entropy less?

Lengths

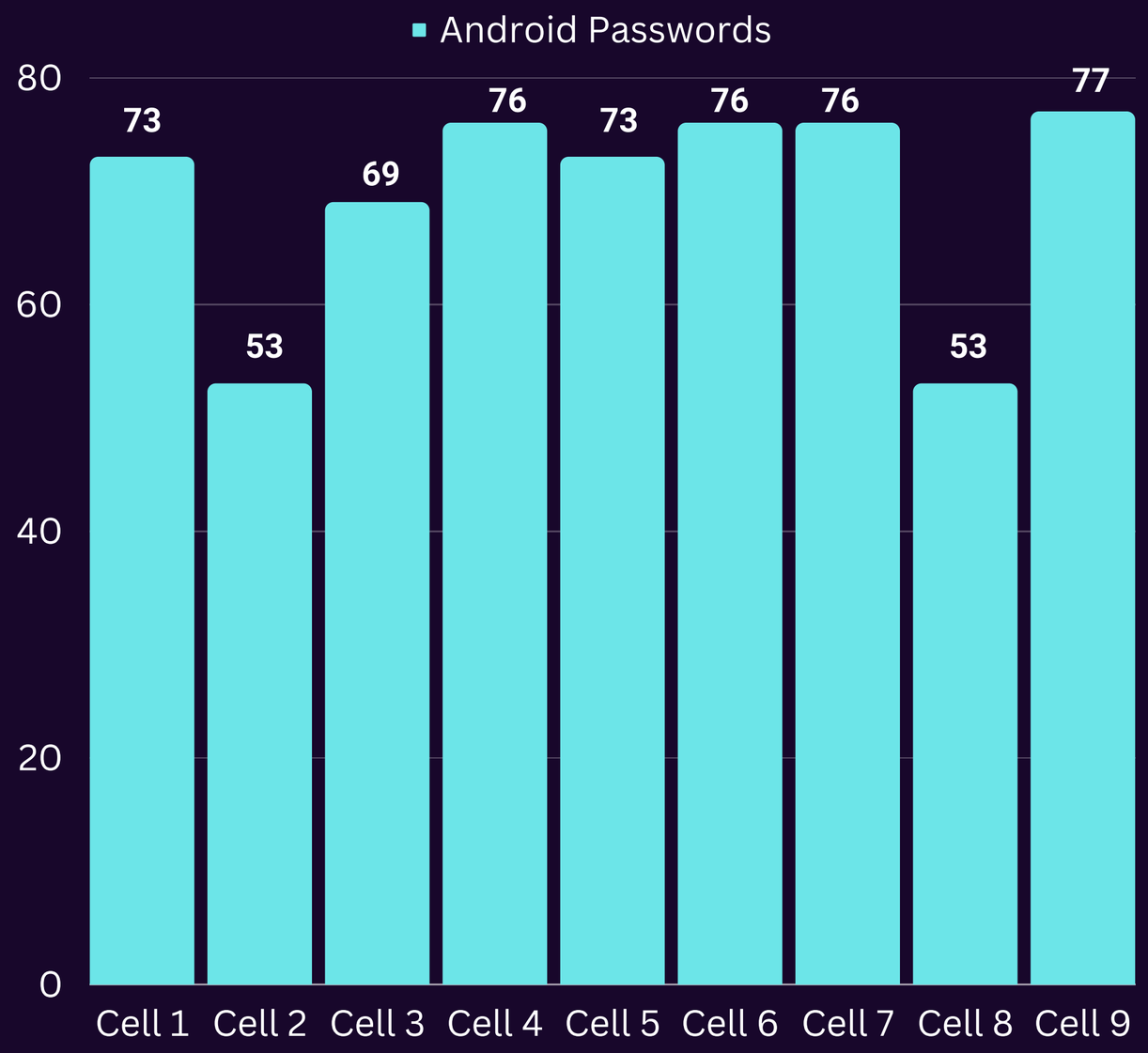
- Medium length passwords tend to be made for android graphical passwords
- Passwords with extreme lengths (either very short or very long) are more likely to be coloured passwords



TRENDS

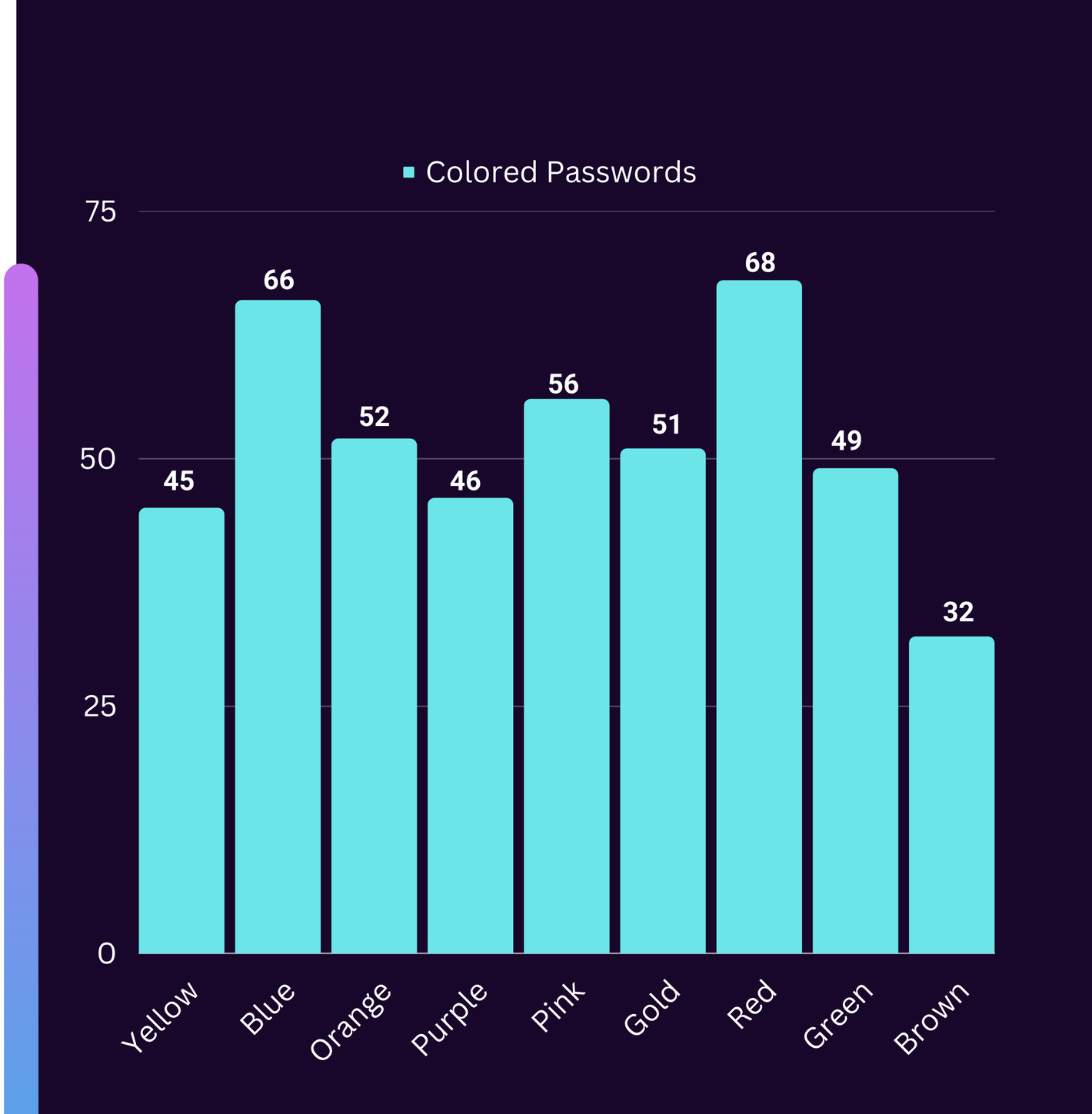
Cell Frequency

- Counts the number of passwords that contain a certain cell
- All of the cells seem to be used by most of the passwords on average, other than Cell 2 and Cell 8 which are considerably lower



Color Frequency

- Counts the number of passwords that contain a color
- Reflects variety found in heat map as well



QUESTIONS?

REFERENCES

[1] Delight-Im. (2014). List of all combinations for the android pattern lock. AndroidPatternLock. Retrieved April 1, 2023, from https://github.com/delight-im/AndroidPatternLock
[2] Dan Goodin - Aug 20, 2015 10:15 am U.T.C. (2015) New data uncovers the surprising predictability of Android Lock Patterns, Ars Technica. Available at: https://arstechnica.com/information-technology/2015/08/new-data-uncovers-the-surprising-predictability-of-android-lock-patterns/ (Accessed: April 2, 2023).

THANK YOU