Password Analysis and Generation

Computational Intelligence Approaches

Assignment Report

Advanced Information Security

Generated: 11/7/2025

Analysis of Password Security using
Random Heuristics vs Markov Chains

Table of Contents

Part 1: Password Database Analysis

2.1 Dataset Overview

Sample Size: 10,000 passwords

Average Length: 11.71 characters

2.2 Statistical Analysis

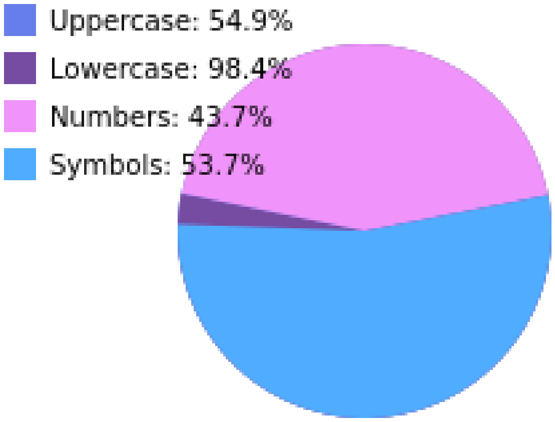
Character Composition:

Uppercase Letters: 54.88%

Lowercase Letters: 98.35%

Numbers: 43.69%

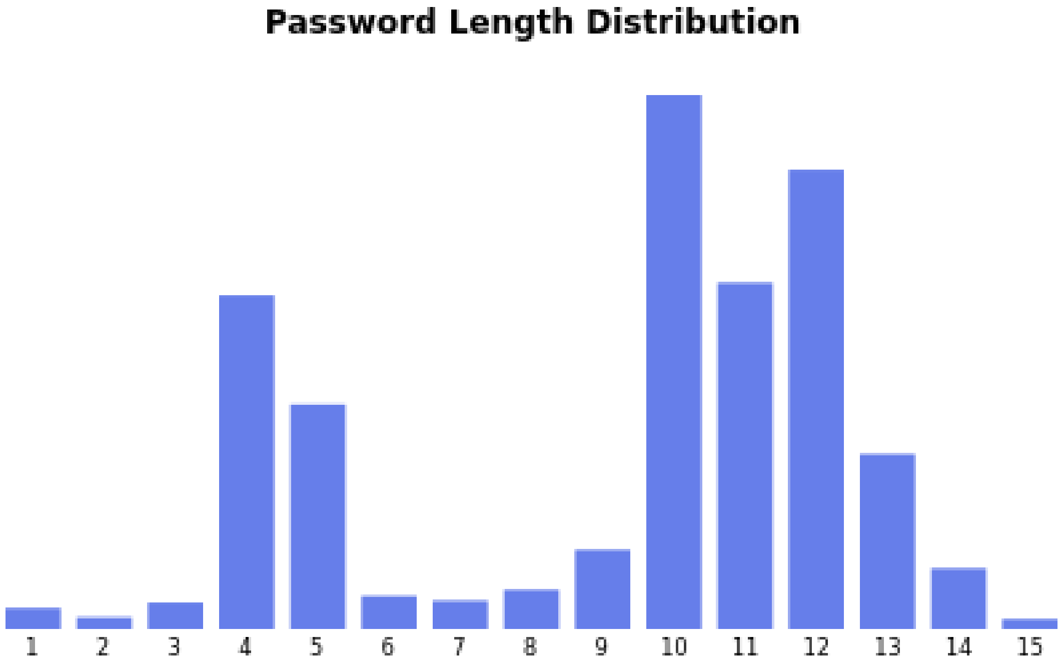
Symbols: 53.66%



2.4 Length Distribution Analysis

Most Common Password Lengths:

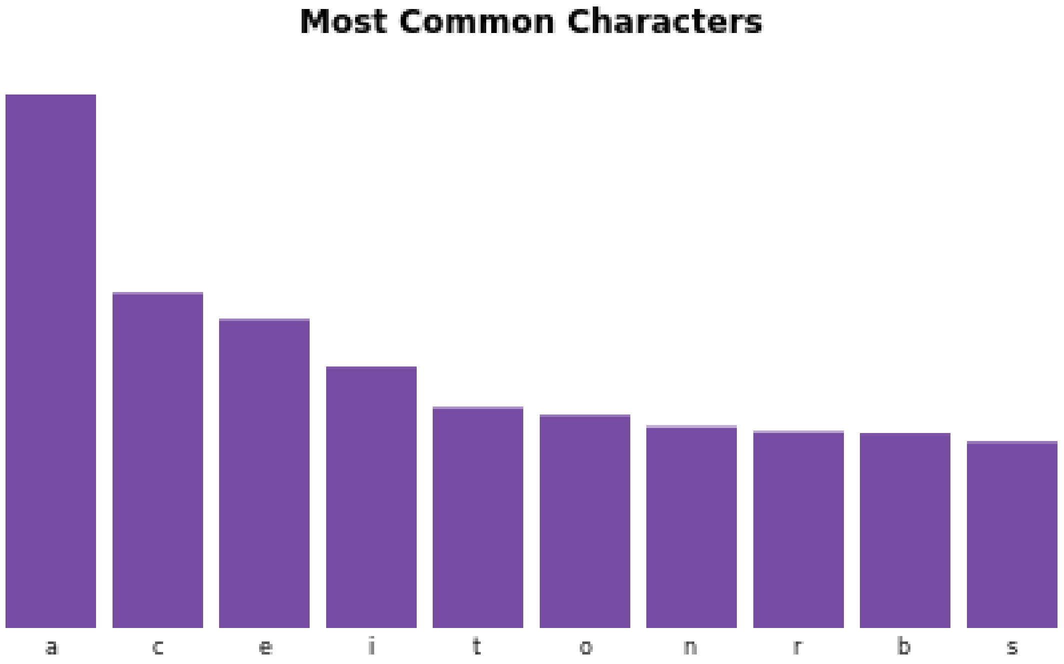
Length 10: 1868 passwords (18.68%)
Length 12: 1606 passwords (16.06%)
Length 11: 1211 passwords (12.11%)
Length 4: 1167 passwords (11.67%)
Length 5: 786 passwords (7.86%)
Length 13: 612 passwords (6.12%)
Length 9: 277 passwords (2.77%)
Length 14: 212 passwords (2.12%)
Length 8: 137 passwords (1.37%)
Length 6: 116 passwords (1.16%)



2.5 Most Common Characters

Top 15 Most Frequent Characters:

'a': 8866 occurrences (88.66%)
'c': 5571 occurrences (55.71%)
'e': 5129 occurrences (51.29%)
'i': 4341 occurrences (43.41%)
't': 3662 occurrences (36.62%)
'o': 3536 occurrences (35.36%)
'n': 3345 occurrences (33.45%)
'r': 3258 occurrences (32.58%)
'b': 3234 occurrences (32.34%)
's': 3092 occurrences (30.92%)
'l': 2925 occurrences (29.25%)
'd': 2756 occurrences (27.56%)
'u': 2453 occurrences (24.53%)
'"': 2234 occurrences (22.34%)
'h': 2091 occurrences (20.91%)



Part 2: Password Generation Analysis

3.1 Random Generator with Heuristics

Configuration:

- Length: 10 characters
- Character set: uppercase, lowercase, symbols
- Avoid similar characters: disabled

- Avoid ambiguous characters: disabled

3.2 Markov Chain Generator

Configuration:

- Model order: 1 (bigrams)
- Training data: 10,000 passwords from PWLDS dataset
- Generation method: probability-based character selection

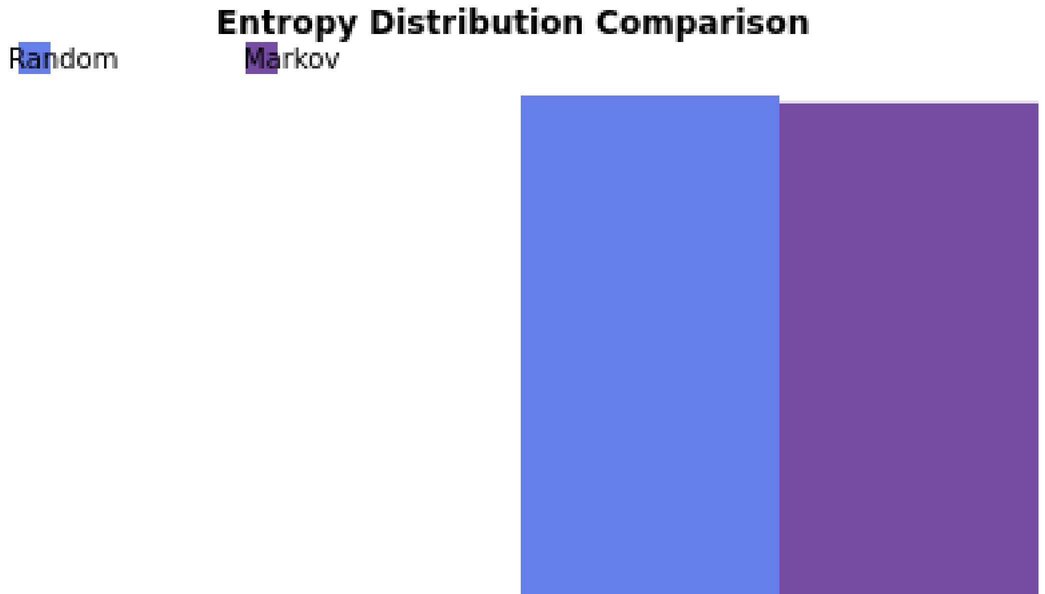
3.3 Comparative Analysis

Entropy Analysis:

Random Generator: 63.92 bits (average)
Markov Generator: 63.85 bits (average)
Difference: -0.07 bits
Better approach: RANDOM

Cracking Time Analysis:

Random Generator: 0.26 years (average)
Markov Generator: 0.26 years (average)
Difference: 0.00 years
Better approach: RANDOM



3.4 Security Metrics Comparison

Security Compliance (60+ bits, 10+ years):

Random Generator:

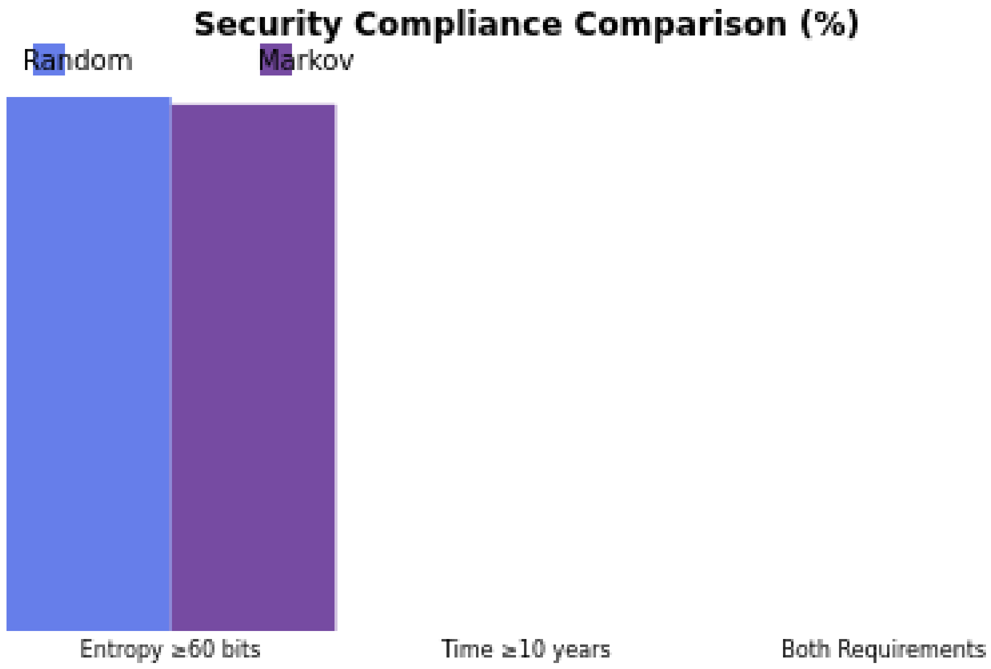
- Entropy more than 60 bits: 100.0%
- Time more than 10 years: 0.0%
- Both requirements: 0.0%

Markov Generator:

- Entropy "e60 bits: 98.6%
- Time "e10 years: 0.0%
- Both requirements: 0.0%

3.5 Readability Analysis

Random Generator: 3.06 (average score)
Markov Generator: 3.67 (average score)
Difference: 0.61
Better approach: MARKOV



4. Conclusions and Recommendations

4.1 Key Findings

Based on the comprehensive analysis of 1,000 generated passwords from each approach:

- RANDOM approach generates passwords with higher average entropy
- RANDOM approach generates passwords with longer average cracking time
- MARKOV approach generates more readable passwords
- RANDOM approach better meets security requirements (60+ bits, 10+ years)

4.2 Recommendations

Based on the analysis, the following recommendations are made:

1. Random approach generates passwords with higher average entropy
2. Random approach generates passwords with longer average cracking time
3. Markov approach generates more readable passwords
4. Random approach better meets security requirements (60+ bits, 10+ years)
5. Overall recommendation: Markov approach is better for this use case

4.3 Overall Winner

MARKOV APPROACH WINS

Scoring:

Random Score: 38.41/100
Markov Score: 40.95/100

The winning approach demonstrates superior performance across multiple security and usability metrics.

5. Appendices

5.1 Sample Generated Passwords

Random Generator (first 10):

1. q=U,uLpY-$ (63.9 bits, 0.3 years)
2. e@RH.&+Dp| (63.9 bits, 0.3 years)
3. em?JT&HwYn (63.9 bits, 0.3 years)
4. njlc%uE-Fb (63.9 bits, 0.3 years)
5. -NwhpDoaRJ (63.9 bits, 0.3 years)
6. -g&ZZ_+)sT (63.9 bits, 0.3 years)
7. tqeG,,q+fl (63.9 bits, 0.3 years)
8. FG-nl{.?JU (63.9 bits, 0.3 years)
9. ,ObAd,tRM+ (63.9 bits, 0.3 years)
10. AT[>zylS]l (63.9 bits, 0.3 years)

Markov Generator (first 10):

1. yO##{?<__? (63.9 bits, 0.3 years)
2. ?jNbss:igy (63.9 bits, 0.3 years)
3. .=Zz:D%Dsi (63.9 bits, 0.3 years)
4. q.agAc.zaa (63.9 bits, 0.3 years)
5. ^adasAbel$ (63.9 bits, 0.3 years)
6. o_Gmicce:u (63.9 bits, 0.3 years)
7. racc@^K+?| (63.9 bits, 0.3 years)
8. eth}^<v]V- (63.9 bits, 0.3 years)
9. abe-s%zpBu (63.9 bits, 0.3 years)
10. Tii!ipou.l (63.9 bits, 0.3 years)