Password Strength Analysis Report

1. Multiple Passwords with Varying Complexity

The following passwords were created and tested with different levels of complexity:

Password	Length	Character Types	Complexity Level
raj1	4	Lowercase, Numbers	Very Weak
raj12	5	Lowercase, Numbers	Weak
raj1234	7	Lowercase, Numbers	Weak
raj1234567	10	Lowercase, Numbers	Moderate
Raj@$125	8	Upper, Lower, Numbers, Symbols	Strong
R@j3$H!92#LmX&	14	Upper, Lower, Numbers, Symbols	Very Strong
Rajesh	6	Uppercase, Lowercase	Weak
Rajesh@754$	11	Upper, Lower, Numbers, Symbols	Strong

---

2. Character Type Variations Used

Uppercase Letters

- Used in: Raj@$125, R@j3$H!92#LmX&, Rajesh, Rajesh@754$
- Purpose: Increases character pool from 26 to 52 letters

Lowercase Letters

- Used in: All passwords
- Purpose: Base alphabetic characters for readability

Numbers

- Used in: raj1, raj12, raj1234, raj1234567, Raj@$125, R@j3$H!92#LmX&, Rajesh@754$
- Purpose: Adds 10 additional characters to the pool

Special Symbols

- Used in: Raj@$125, R@j3$H!92#LmX&, Rajesh@754$
- Symbols used: @, $, !, #, &
- Purpose: Dramatically increases complexity and character pool

Length Variations

- Shortest: 4 characters (raj1)
- Longest: 14 characters (R@j3$H!92#LmX&)
- Range: 4-14 characters

---

3. Password Strength Test Results

Password Analysis Summary

raj1 (4 characters)

- **Estimated Strength**: Very Weak
- **Crack Time**: Less than 1 second
- **Issues**: Too short, no uppercase, no symbols, dictionary word base

raj12 (5 characters)

- **Estimated Strength**: Weak
- **Crack Time**: Less than 1 second
- **Issues**: Too short, no uppercase, no symbols, predictable pattern

raj1234 (7 characters)

- **Estimated Strength**: Weak
- **Crack Time**: Seconds to minutes
- **Issues**: Sequential numbers, no uppercase, no symbols

raj1234567 (10 characters)

- **Estimated Strength**: Moderate
- **Crack Time**: Hours to days
- **Issues**: Predictable sequential pattern, no uppercase or symbols

Raj@$125 (8 characters)

- **Estimated Strength**: Strong
- **Crack Time**: Months to years
- **Strengths**: Mixed case, symbols, numbers

- **Issues**: Still contains recognizable word "Raj"

R@j3$H!92#LmX& (14 characters)

- **Estimated Strength**: Very Strong
- **Crack Time**: Centuries
- **Strengths**: Long length, all character types, no patterns

Rajesh (6 characters)

- **Estimated Strength**: Weak
- **Crack Time**: Minutes
- **Issues**: Common name, no numbers or symbols, too short

Rajesh@754$ (11 characters)

- **Estimated Strength**: Strong
- **Crack Time**: Years
- **Strengths**: Good length, mixed characters
- **Issues**: Contains dictionary word (name)

---

4. Scores and Feedback Summary

Key Findings from Password Strength Checker

Common Feedback Received:

- Passwords under 8 characters are considered weak
- Using only lowercase and numbers provides minimal security
- Sequential patterns (1234567) are easily guessable
- Dictionary words or names reduce strength significantly
- Symbols and mixed case dramatically improve strength
- Length is one of the most important factors

Scoring Pattern Observed:

- 0-25%: Very Weak (raj1, raj12)
- 26-50%: Weak (raj1234, Rajesh)
- 51-75%: Moderate to Strong (raj1234567, Raj@$125, Rajesh@754$)

- 76-100%: Very Strong (R@j3$H!92#LmX&)

---

5. Best Practices for Creating Strong Passwords

Essential Requirements

1. **Minimum Length**
    - Use at least 12 characters
    - 14+ characters recommended for critical accounts
    - Each additional character exponentially increases security
2. **Character Diversity**
    - Include uppercase letters (A-Z)
    - Include lowercase letters (a-z)
    - Include numbers (0-9)
    - Include special symbols (@, #, $, !, &, %, etc.)
3. **Avoid Common Patterns**
    - No sequential numbers (123456)
    - No keyboard patterns (qwerty, asdfgh)
    - No repeated characters (aaaaaa)
    - No simple substitutions (P@ssw0rd)
4. **Avoid Personal Information**
    - No names (yours or family members)
    - No birthdates
    - No phone numbers
    - No addresses
    - No pet names
5. **Uniqueness**
    - Use different passwords for different accounts
    - Never reuse passwords across important sites
    - Don't use slight variations of the same password

Advanced Best Practices

6. **Randomness**

- Use password generators for maximum randomness
- Avoid predictable word combinations
- Mix character positions unpredictably

7. **Memorability vs Security Balance**
   - Use passphrases: "Coffee$Morning#Beach!2024"
   - Create acronyms from sentences: "IW2EbCo@8AM!" (I Wake 2 Eat breakfast Coffee @ 8 AM!)
   - Use password managers to store complex passwords
8. **Regular Updates**
   - Change passwords every 90-180 days for critical accounts
   - Change immediately if breach is suspected
   - Don't reuse old passwords

---

6. Key Tips Learned from Evaluation

Critical Lessons

1. **Length Matters Most**
   - A 12-character password with basic complexity beats an 8-character password with high complexity
   - Each added character multiplies crack time exponentially
2. **Character Variety is Essential**
   - Using all four character types (upper, lower, number, symbol) creates the strongest passwords
   - Even one symbol dramatically increases strength
3. **Predictable Patterns Are Dangerous**
   - Common patterns like "123456" or "password" are cracked instantly
   - Even longer passwords with patterns (raj1234567) remain vulnerable
4. **Names and Dictionary Words Reduce Security**
   - Attackers use dictionary attacks that include common names
   - "Rajesh" alone is weak, but "R@j3$H!92#LmX&" is very strong
5. **Context Matters**
   - Banking/email passwords need maximum strength
   - Less critical accounts can use moderate strength
   - Never use weak passwords for any online account

Practical Implementation Tips

- **Use a Password Manager**: LastPass, 1Password, Bitwarden, or Dashlane
- **Enable Two-Factor Authentication (2FA)**: Adds extra security layer
- **Test Before Using**: Always check strength before finalizing
- **Write Down Securely**: If needed, store in physical safe, not digitally
- **Update Regularly**: Set calendar reminders for password changes

---

7. Common Password Attacks

1. Brute Force Attack

Description: A brute force attack systematically tries every possible combination of characters until the correct password is found.

How It Works:

- Starts with single characters: a, b, c... 1, 2, 3...
- Progresses to two characters: aa, ab, ac... a1, a2...
- Continues through all combinations
- Eventually tries every possible password

Time to Crack Examples:

- 4-character password (lowercase only): < 1 second
- 8-character password (lowercase only): 7 hours
- 8-character password (all character types): 7 years
- 12-character password (all character types): 34,000 years

Defense:

- Use long passwords (12+ characters)
- Use all character types
- Account lockout policies (limit login attempts)
- Rate limiting on login attempts

2. Dictionary Attack

Description: Uses a pre-compiled list of common words, phrases, names, and commonly used passwords.

How It Works:

- Tries words from dictionaries (English, multilingual)
- Tests common passwords (password, 123456, qwerty)
- Includes names, places, sports teams
- Uses leaked password databases
- Tries common substitutions (P@ssw0rd, Pa$$word)

Common Dictionary Sources:

- RockYou database (32 million real passwords)
- SecLists password lists
- Wikipedia word lists
- Common names databases

Defense:

- Avoid dictionary words
- Don't use names or common phrases
- Use random character combinations
- Implement account lockout mechanisms

3. Rainbow Table Attack

Description: Uses pre-computed hash tables to reverse cryptographic hash functions.

How It Works:

- Hashes are mathematical one-way functions
- Rainbow tables contain millions of pre-computed password hashes
- Attackers compare stolen hashes against tables
- Instant match reveals original password

Defense:

- Salting (adding random data before hashing)
- Using strong hashing algorithms (bcrypt, Argon2)
- Long, complex passwords are harder to pre-compute

4. Credential Stuffing

Description: Uses username/password combinations from previous data breaches.

How It Works:

- Hackers obtain credentials from breached websites
- Try same credentials on other sites
- Works because people reuse passwords
- Automated tools test millions of combinations

Defense:

- Use unique passwords for each account
- Enable breach monitoring (Have I Been Pwned)
- Use password managers to generate unique passwords

5. Phishing Attacks

Description: Tricks users into revealing passwords through deception.

How It Works:

- Fake login pages mimicking legitimate sites
- Emails pretending to be from trusted sources
- Social engineering to manipulate users
- Users voluntarily enter passwords

Defense:

- Verify website URLs carefully
- Never click email links requesting passwords
- Enable 2FA to protect even if password is stolen
- Security awareness training

6. Keylogger Attacks

Description: Malware records every keystroke on infected computers.

How It Works:

- Software or hardware records all typing
- Captures passwords as they're typed

- Sends data to attacker
- Works regardless of password strength

Defense:

- Anti-malware software
- Virtual keyboards for sensitive logins
- Password managers (auto-fill avoids typing)
- Regular system scans

---

8. How Password Complexity Affects Security

Mathematical Foundation

Character Pool Size:

- Lowercase only (26 characters): 26^n possible combinations
- - Uppercase (52 characters): 52^n possible combinations
- - Numbers (62 characters): 62^n possible combinations
- - Symbols (92+ characters): 92^n possible combinations

Where n = password length

Exponential Growth:

- 8-char lowercase: 208,827,064,576 combinations
- 8-char all types: 6,095,689,385,410,816 combinations
- 12-char all types: 475,920,314,814,253,376,475,136 combinations

Real-World Impact

Time to Crack Analysis

4-Character Password:

- Lowercase only: < 1 second
- All character types: < 1 second
- **Verdict**: Unacceptable for any use

8-Character Password:

- Lowercase only: 7 hours
- All character types: 7 years
- **Verdict**: Minimum acceptable with all character types

12-Character Password:

- Lowercase only: 2 months
- All character types: 34,000 years
- **Verdict**: Strong security for most purposes

16-Character Password:

- Lowercase only: 5 years
- All character types: 44 million years
- **Verdict**: Excellent security

Security Improvement Factors

Adding One Character:

- Multiplies crack time by character pool size (26-92x)
- More effective than adding complexity to shorter password

Adding Character Type:

- Lowercase → + Uppercase: 2x improvement
- - Numbers: 2.4x improvement
- - Symbols: 1.5x improvement
- **Combined effect**: 7.2x improvement for 8-char password

Removing Patterns:

- Dictionary words: Reduces from years to seconds
- Sequential patterns: Reduces by 99%+
- Personal info: Makes vulnerable to targeted attacks

Practical Security Implications

Low Complexity (raj1234)

- **Crack Time**: Minutes

- **Attack Success**: 100% with dictionary attack
- **Risk Level**: Critical
- **Acceptable Use**: Never

Moderate Complexity (raj1234567)

- **Crack Time**: Hours to days
- **Attack Success**: High with pattern recognition
- **Risk Level**: High
- **Acceptable Use**: Low-security local applications only

High Complexity (Raj@$125)

- **Crack Time**: Months to years
- **Attack Success**: Low with brute force
- **Risk Level**: Moderate
- **Acceptable Use**: Most online accounts with 2FA

Maximum Complexity (R@j3$H!92#LmX&)

- **Crack Time**: Centuries
- **Attack Success**: Nearly impossible
- **Risk Level**: Minimal
- **Acceptable Use**: All purposes including banking

Defense-in-Depth Strategy

Password complexity is part of layered security:

1. **Strong Password**: First line of defense
2. **Two-Factor Authentication**: Protects even if password compromised
3. **Account Monitoring**: Detect suspicious access
4. **Regular Updates**: Limit damage from undetected breaches
5. **Unique Passwords**: Contain breach to single account
6. **Password Manager**: Enable use of maximum complexity

Conclusion on Complexity Impact

Password complexity doesn't just improve security incrementally—it creates exponential improvements. A 12-

character password with all character types is not slightly better than an 8-character one; it's millions of times more secure. The combination of length and character diversity creates a multiplicative effect that transforms a password from crackable in seconds to effectively unbreakable.

The Security Equation:

```
Security = (Character Pool Size)^Length × Pattern Randomness
```

Every element must be maximized for true security. A long password with patterns is weak. A complex password that's too short is weak. Only the combination of adequate length (12+), full character diversity (4 types), and randomness (no patterns) creates truly secure passwords.

Final Recommendations

For Immediate Implementation

1. **Audit Current Passwords**: Check all passwords against strength criteria
2. **Replace Weak Passwords**: Prioritize banking, email, and social media
3. **Install Password Manager**: Use to generate and store strong passwords
4. **Enable 2FA**: Add second authentication factor wherever available
5. **Check for Breaches**: Use haveibeenpwned.com to check email addresses

Password Creation Formula

Minimum Standard:

- 12+ characters
- At least one uppercase letter
- At least one lowercase letter
- At least one number
- At least one special symbol
- No dictionary words or names
- No sequential patterns
- Unique for each account

Example Strong Password Generation:

1. Start with random words: "Sunset Mountain Coffee"

2. Take first letters: "SMC"
3. Add random numbers: "SMC8729"
4. Add symbols: "S@MC#8729"
5. Extend and randomize: "S@MC#8729!Bx&Pm"
6. Result: 16-character strong password

Long-Term Security Culture

- Treat passwords as keys to your digital life
- Never share passwords via email, text, or verbally
- Change passwords immediately after suspected compromise
- Educate family members about password security
- Regular security training and awareness
- Stay informed about new security threats

Report Prepared By: Adarsh R Majigoudar

Date: 2025

Classification: Educational Document

Purpose: Password Security Awareness and Best Practices