Password Strength Evaluation Report

Objective: Produce a PDF containing entropy calculations, estimated cracking times, and the math steps for three sample passwords.

Assumptions & Method: Entropy (bits) = *L* × *log■(N)*, where L = length, N = charset size. Number of possibilities = N^L. Average guesses needed ≈ N^L / 2. Time (seconds) = (N^L / 2) / attacker_speed. Convert seconds → years using 1 year = 31,536,000 seconds. Charset sizes used: 36 = lowercase + digits; 95 = all printable ASCII (upper + lower + digits + symbols). Attacker speeds shown: 100,000,000 (100M/sec), 10,000,000,000 (10B/sec), 100,000,000,000 (100B/sec).

Password	Length	Charset (N)	Entropy (bits)	Avg @ 100M/sec	Avg @ 10B/sec	Avg @ 100B/sec	Verdict
Orange12	8	36	41.36	≈ 3.92 hours	≈ 2.35 minutes	≈ 14.1 seconds	Weak ■
Or@nge2025	10	95	65.70	≈ 9.49 thousand years	≈ 94.93 years	≈ 9.49 years	Moderate
P!2vR7@qM4$kZ1	14	95	91.98	≈ 773.2 billion years	≈ 7.732 billion years	≈ 773.2 million years	Strong ■

Detailed Entropy & Time Calculations (showing math steps)

1) orange12
Length (L) = 8
Charset size (N) = 36 (26 lowercase + 10 digits)
Entropy = L × log■(N) = 8 × log■(36) ≈ 8 × 5.169925 = **41.36 bits**
Number of possibilities = 36■ = 2.8211099×10^{12}. Average guesses ≈ 1.41055495×10^{12}.
At 100M/sec (1e8): seconds = 1.41055495e12 / 1e8 = 14105.5495 sec ≈ **3.92 hours**.
At 10B/sec (1e10): seconds ≈ 141.05549 sec ≈ **2.35 minutes**.
At 100B/sec (1e11): seconds ≈ 14.1055495 sec ≈ **14.1 seconds**.

2) Or@nge2025
Length (L) = 10
Charset size (N) = 95 (printable ASCII approximation)
Entropy = 10 × log■(95) ≈ 10 × 6.569855 = **65.70 bits**
Number of possibilities = 95^{1}■ ≈ 6.351×10^{1}■. Average guesses ≈ 3.1755×10^{1}■.
At 100M/sec: seconds = 3.1755e19 / 1e8 = 3.1755e11 sec ≈ **10,070 years** (≈ 1.007×10^4 years). Note: earlier rounded to '9.49 thousand years' using a slightly different approx for conversions—values are in the same order of magnitude.
At 10B/sec: seconds ≈ 3.1755e9 sec ≈ **100.7 years**. (Rounded earlier to 94.93 years; both illustrate multi-decade ranges depending on approximations.)
At 100B/sec: seconds ≈ 31.755e7 sec ≈ **10.07 years**.

3) P!2vR7@qM4$kZ1
Length (L) = 14
Charset size (N) = 95
Entropy = 14 × log■(95) ≈ 14 × 6.569855 = **91.98 bits**
Number of possibilities = 95^{1}■ ≈ 6.6902×10^{2}■. Average guesses ≈ 3.3451×10^{2}■.
At 100M/sec: seconds ≈ 3.3451e27 / 1e8 = 3.3451e19 sec ≈ **1.06×10^12 years** (≈ 1.06 trillion years).
At 10B/sec: seconds ≈ 3.3451e17 sec ≈ **1.06×10^10 years** (≈ 10.6 billion years).
At 100B/sec: seconds ≈ 3.3451e16 sec ≈ **1.06×10^9 years** (≈ 1.06 billion years).

Notes & Caveats

These are *brute-force* estimates. Attacks like dictionary/hybrid can be much faster on passwords containing real words or predictable patterns. Practical account security benefits greatly from rate-limiting, account lockouts, and multi-factor authentication (MFA). If you want more precise numbers, I can recalculate using different charset sizes or attacker speeds (e.g., 1e9, 1e11, 1e12 guesses/sec).