Task 6 — Password Table View and Explanation

#	Password Type	Example (masked)	Length	Character Types	Strength (Tool)	Feedback
1	Very Weak	*********	8–9	Lowercase only	Very Weak	Common word, easy to guess
2	Weak + Number	********21	10–11	Lowercase + digits	Weak	Still predictable
3	Moderate	S*******92	10–11	Upper/lowercase + digits	Moderate	Improved, but short
4	Strong	S*!*******23	12+	Upper/lower/digits/symbols	Strong	Good complexity
5	Passphrase	blue horse ****	16+	Words + spaces/symbols	Strong	Long and memorable
6	Random High-Entropy	g*&J*********X	16+	Mixed all types	Very Strong	High entropy, secure

Explanation:
The table illustrates the difference between weak, moderate, and strong password types. Simple words scored very poorly because they are vulnerable to dictionary attacks. Adding digits and uppercase improved results slightly, but still left them short and guessable. Longer passphrases showed strong ratings due to length and unpredictability. The random high-entropy password scored the highest, proving that both *length* and *complexity* make passwords highly resistant to brute-force attacks.

— End of Table View —