

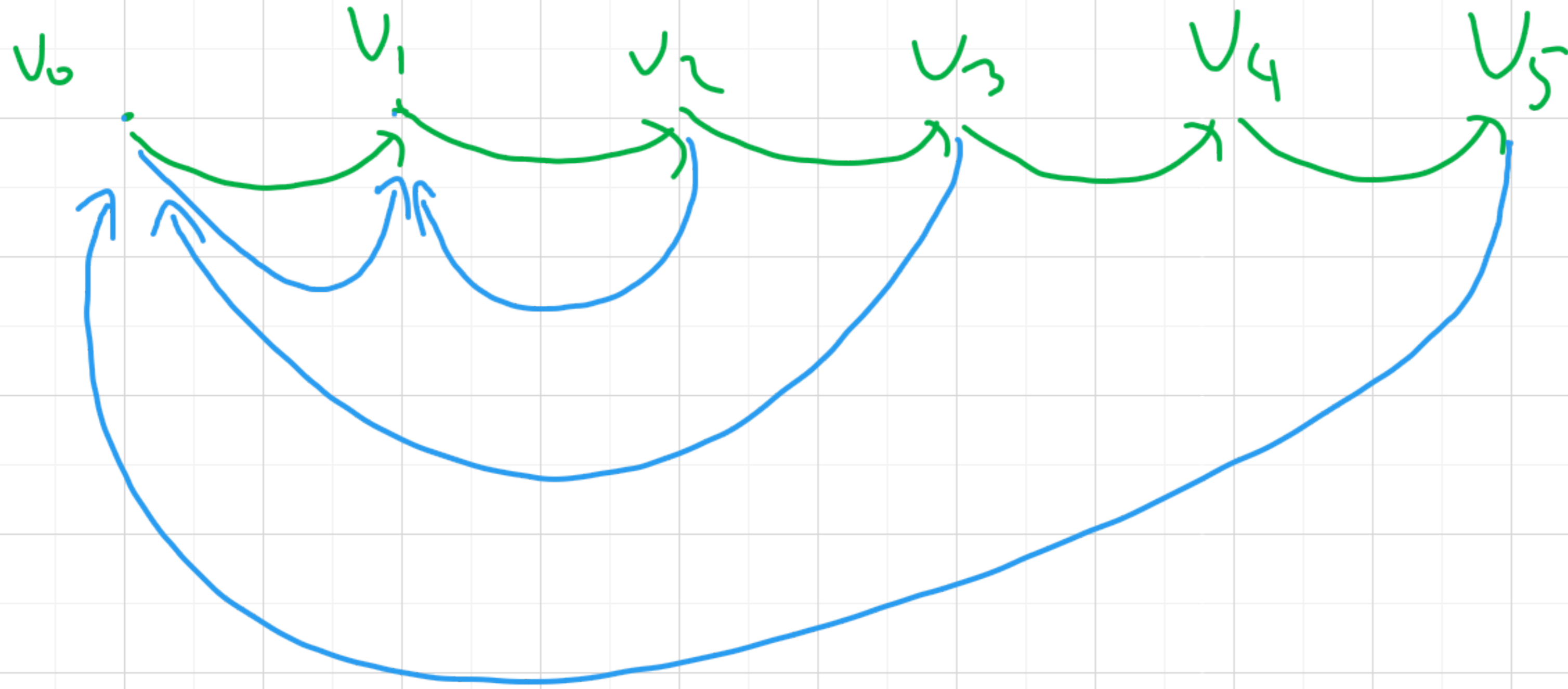
Web APP Security ||

PBKDF (Password Based Key Derivation F.)



$$v_n = \text{PKDF-?}(\text{pass})$$
$$= h^n(\text{pass})$$

SCRIPT



$$\cdot v_0 \bmod 6 = 3 \rightarrow$$
$$v_0 \leftarrow F(v_5 \oplus v_3)$$

$$v_1 \bmod 3 = 2$$
$$v_1 \leftarrow F(v_0 \oplus v_2)$$

