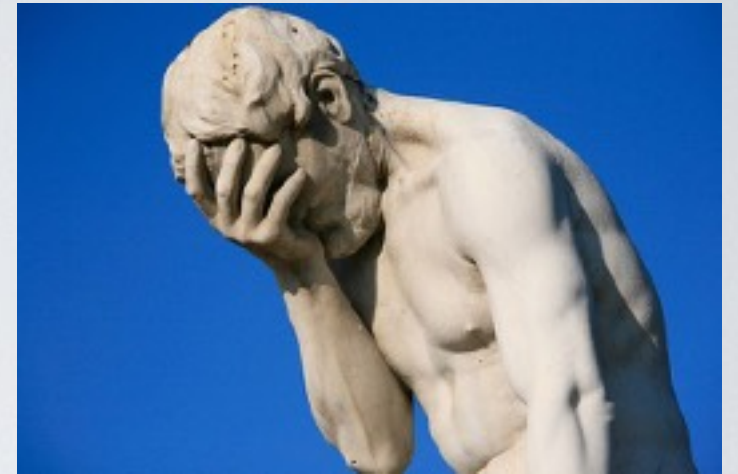


# WEP - Wired Equivalent Privacy



- ➡ A random number IV (24 bits only) transmitted in clear between the clients and the base station

$$\text{RC4\_key} = \text{IV} + \text{SSID\_password}$$

- ⦿ 50% chance the same IV will be used again after 5000 packets

# Salsa20 (and ChaCha20)

Key Size	128 or 256 bits
Speed	~ 4 cycles / byte