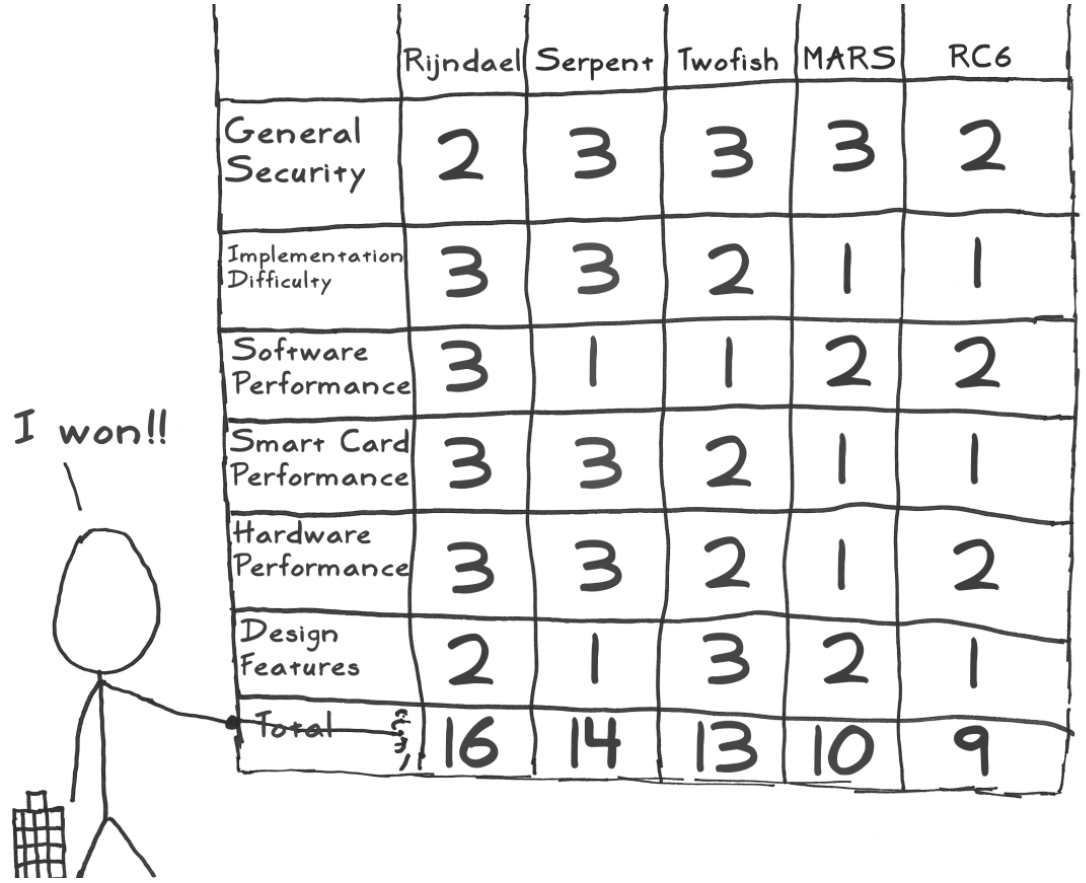
storia AES

- nel settembre 97 il NIST comincia la selezione del successore del DES
- si chiamerà AES – Advanced Encryption Standard
- 21 proposte - solo 15 soddisfano i criteri necessari
- i 15 candidati vengono annunciati nella *First AES Candidate Conference*, nel 98
- seguono la *Second AES Candidate Conference*, a Roma nel 99, dopo la quale vengono annunciati i 5 finalisti
- sono MARS, RC6, Rijndael, Serpent, Twofish
- la *Third AES Candidate Conference* si tiene nel'aprile 2000
- nell'ottobre 2000 viene scelto Rijndael

- la competizione è stata molto internazionale
- Rijndael è stato proposta da due crittografi belgi: Daemen e Rijmen
- MARS (IBM), RC6 (Rivest e RSA Security), Twofish (Schneier e altri)
- Serpent è di Anderson (UK), Biham (Israele), Knudsen (Danimarca)



(illustrazione di Jeff Moser da `http://www.moserware.com`)