

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 nell'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)

I won!!



	Rijndael	Serpent	Twofish	MARS	RC6
General Security	2	3	3	3	2
Implementation Difficulty	3	3	2	1	1
Software Performance	3	1	1	2	2
Smart Card Performance	3	3	2	1	1
Hardware Performance	3	3	2	1	2
Design Features	2	1	3	2	1
Total	16	14	13	10	9

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