

# Estimated Complexity of brute-force attack on AES



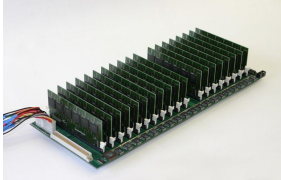

September 1st, 2009

Keylength (bit)	possible Keys ( $2^{\text{Keylength}}$ )	possible Keys ( $2^{\text{Keylength}}$ )	Multiples of 32bit
32	4294967296	4.294.967.296	1
48	2,81475E+14	281.474.976.710.656	65.536
64	1,84467E+19	18.446.744.073.709.600.000	4.294.967.296
128	3,40282E+38	340.282.366.920.938.000.000.000.000.000.000.000.000.000	79.228.162.514.264.300.000.000.000.000

Gflop to break AES32 840

Time for brute force computation of all possible keys				
system	Pentium4	Core i7	COPACOBANA	Roadrunner
Gflop/s	14	50	115.000	1.105.000
Keylength (bit)				
32	1 min	17 s	73 ms	76 $\mu$ s
48	46 d	13 d	8 min	5 s
64	8.172 y	2.288 y	1 y	4 d
128	150.738.513.154.993.000.000.000 y	42.206.783.683.398.100.000.000 y	18.350.775.514.520.900.000 y	190.035.045.850.509.000 y

### Different Calculation Power

system	Pentium4	Core i7	COPACOBANA	Roadrunner
				
Intels well known Pentium 4 processor Instruction Set 64-bit Price \$59.00	Intels latest processor for desktop computing Launch Date Q2'09 Processor Number i7-975 # of Cores 4 Clock Speed 3.333 GHz Intel® Smart Cache 8 MB Bus/Core Ratio 25 Intel® QPI Speed 6.4 GT/s # of QPI Links 1 Instruction Set 64-bit 1ku Bulk Budgetary Price \$999.00	COPACOBANA, the Cost-Optimized Parallel COde Breaker, is an FPGA-based machine which is optimized for running cryptanalytical algorithms. COPACOBANA is suitable for parallel computation problems which have low communication requirements. Any symmetric cipher with up to roughly 64 key bits can be attacked with COPACOBANA. Examples include RCS or GSM A5. Moreover, presumably strong ciphers with a long theoretical key size can be broken if the number of required steps is less than $2^{64}$ . COST: appr.EUR 10.000,-	Roadrunner is a supercomputer built by IBM at the Los Alamos National Laboratory in New Mexico, USA. Currently the world's fastest computer, the US\$133-million Roadrunner is designed for a peak performance of 1.7 petaflops, achieving 1.026 on May 25, 2008	

**Gflop/s** is a rate of execution, billions of floating point operations per second. Whenever this term is used it will refer to 64 bit floating point operations and the operations will be either addition or multiplication.

Albania, Austria, Belarus, Bosnia & Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Estonia, Greece, Hungary, Kazakhstan, Kosovo, Latvia, Liechtenstein, Lithuania, Macedonia, Montenegro, Poland, Romania, Russia, Serbia, Slovak Rep., Slovenia, Switzerland, Turkey, Ukraine