NIST's Preliminary Testing of AES Candidates

- Cost (Efficiency)
  - Encryption / Decryption Speeds
  - Key Setup Times
- NIST Platform
  - IBM-compatible PC; Intel Pentium Pro Processor, 200MHz, 64MB RAM, Windows95 (v 4.00.950 B)
- Testing performed using Optimized ANSI C code provided by AES algorithm submitters

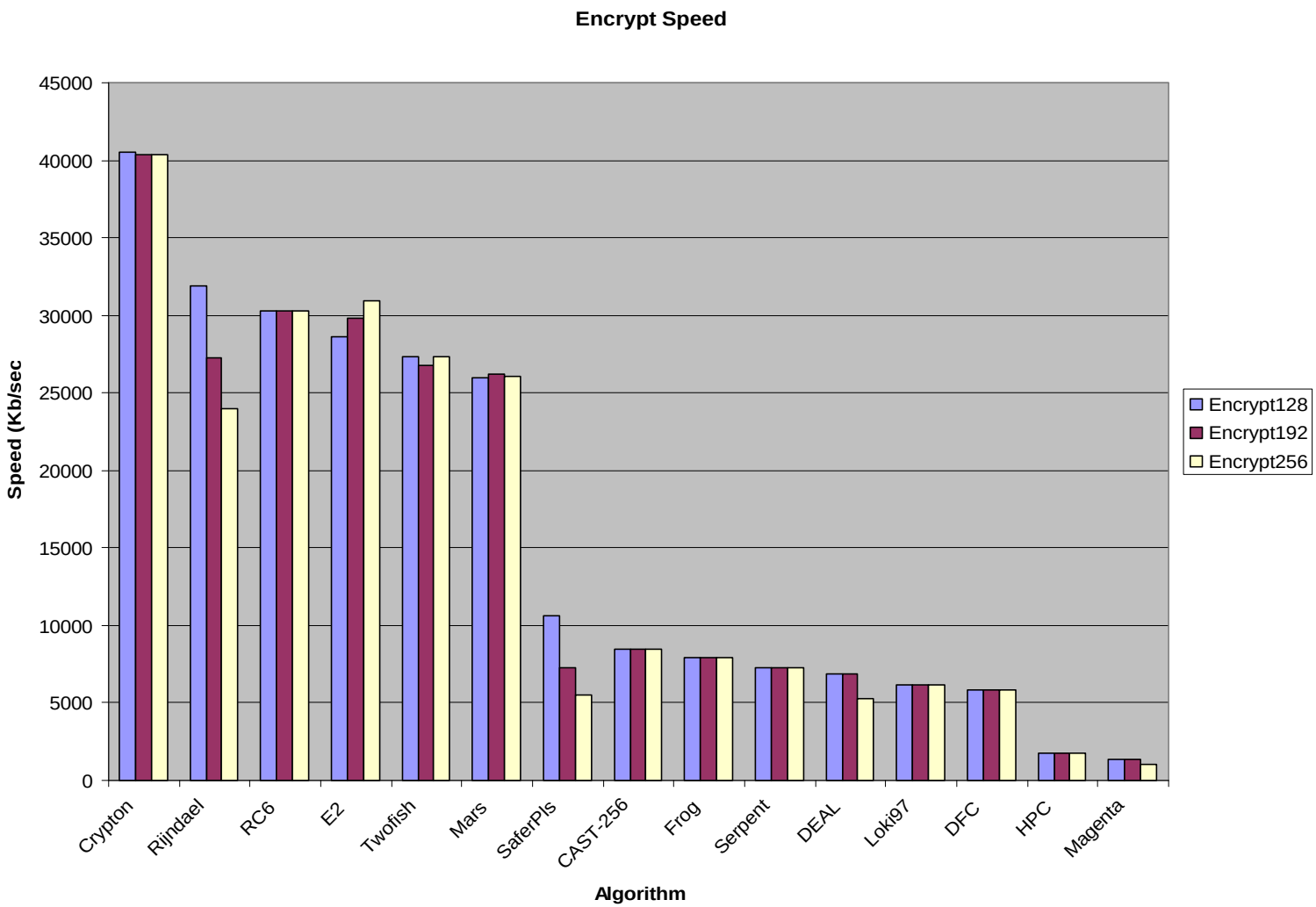
Disclaimer

- These are *preliminary* testing results, for one specific platform (200MHz PC w/ Pentium Pro). Testing is being performed on multiple platforms, using *multiple compilers*. Therefore, the following slides do NOT reflect all of NIST's efficiency testing.

- The following slides do NOT reflect other efficiency testing performed by public evaluators/testers.

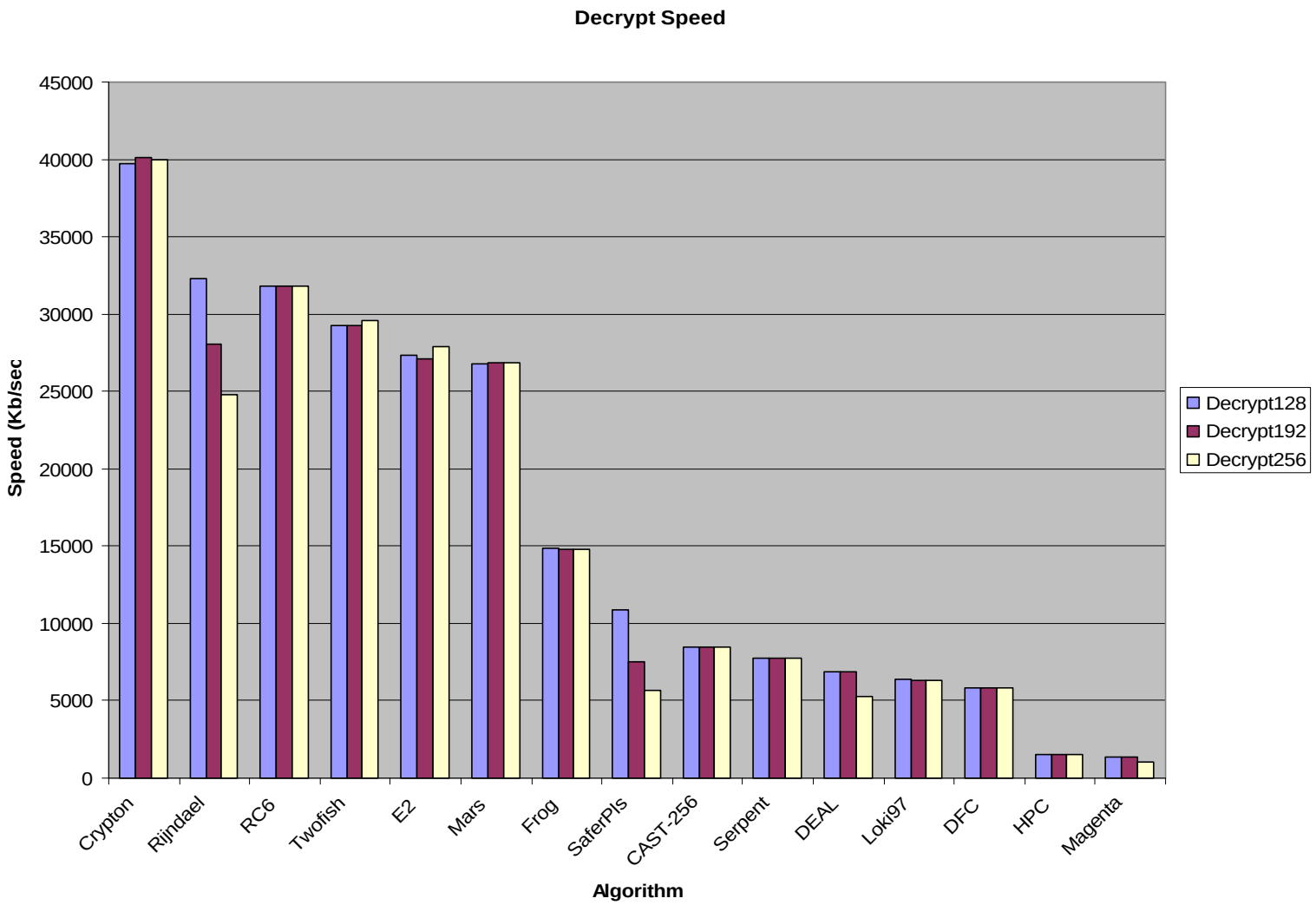
- Keep in mind that there are **many** factors in addition to NIST's efficiency testing which will be used to select the candidates for Round 2.

Encryption Speeds on NIST Platform



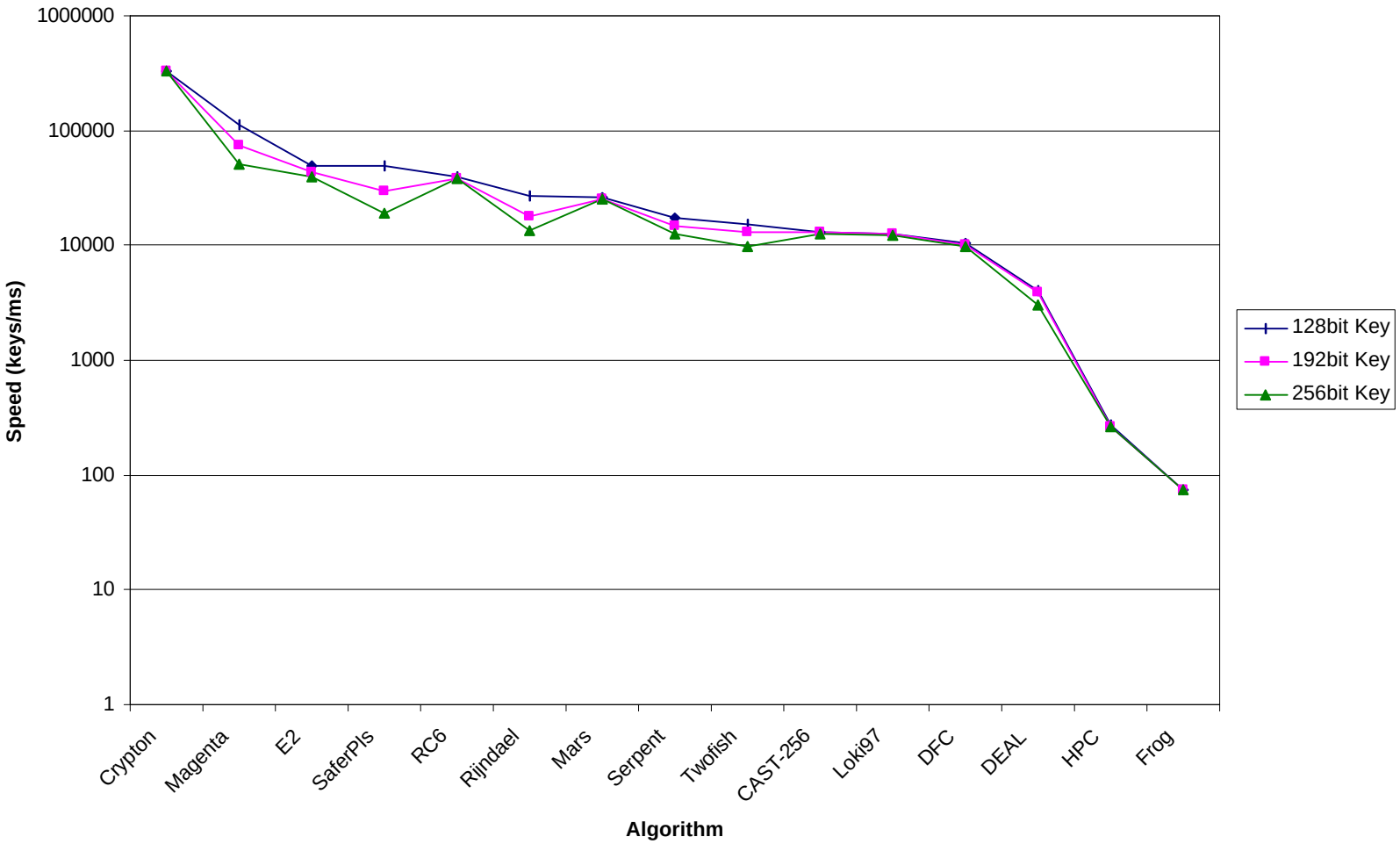
*Compiler: Borland C++ 5.0 (options: -Oi -6 -v -A -a4 -O2)

Decryption Speeds on NIST Platform

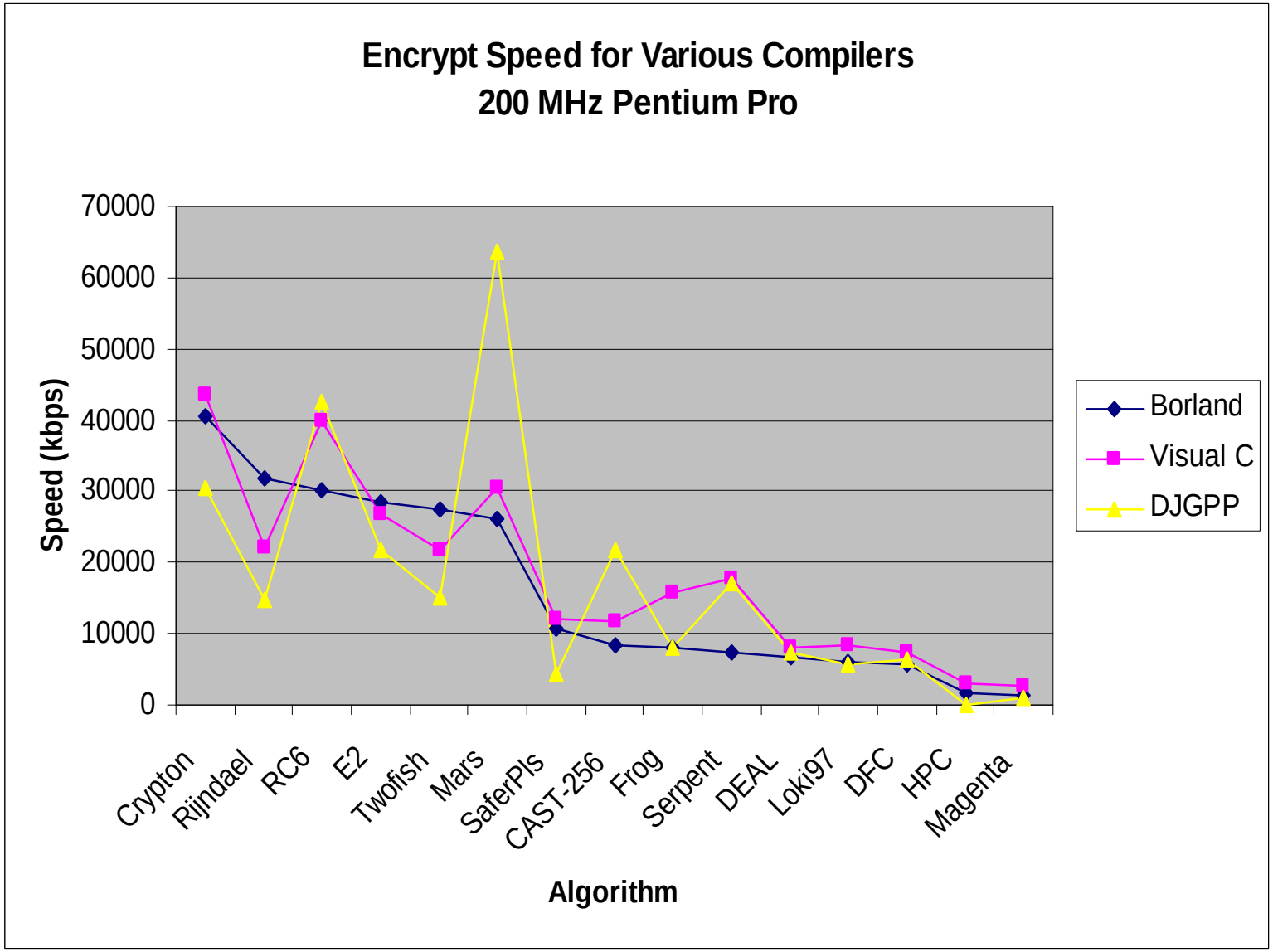


*Compiler: Borland C++ 5.0 (options: -Oi -6 -v -A -a4 -O2)

Key Setup Speeds on NIST Platform



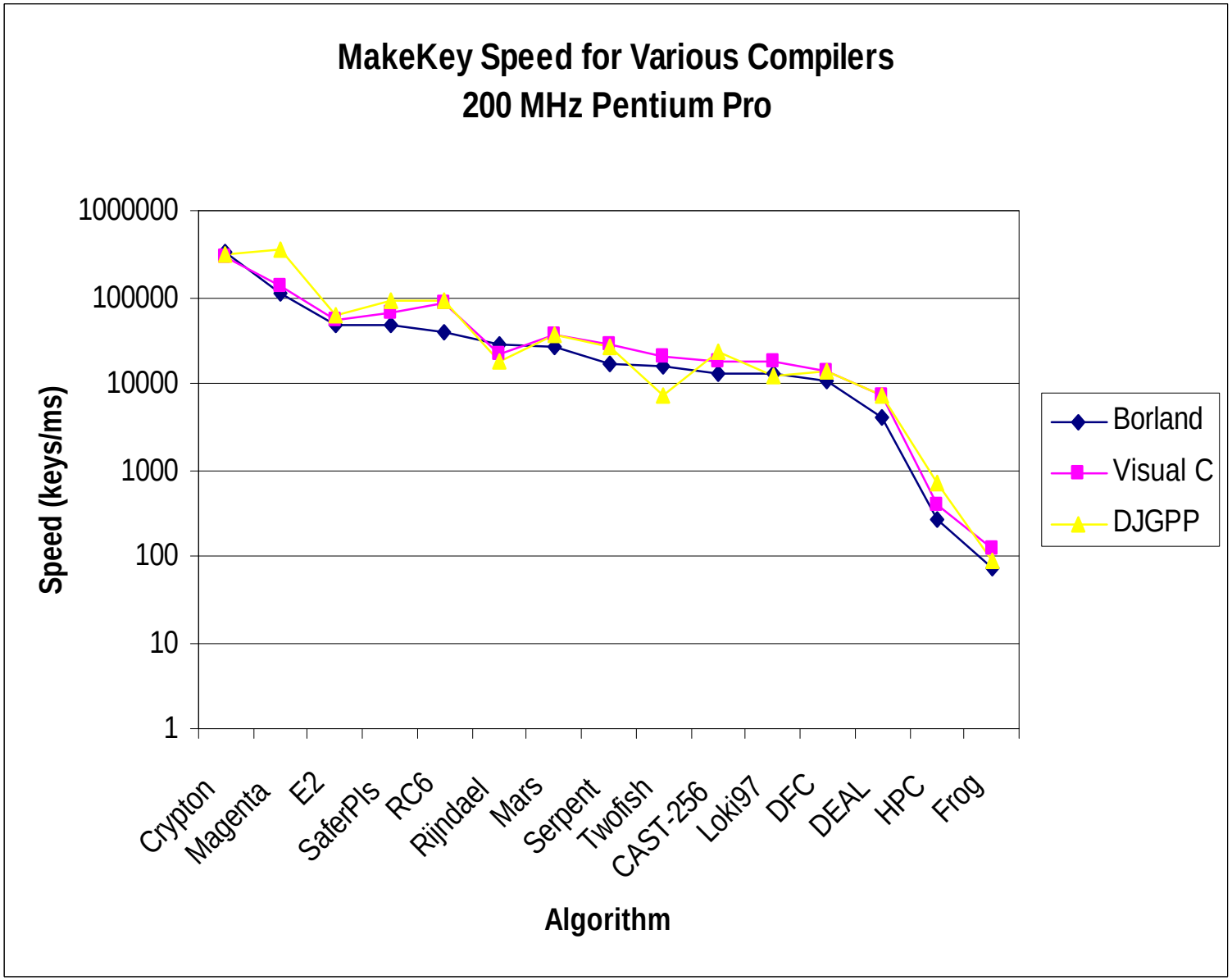
*Compiler: Borland C++ 5.0 (options: -Oi -6 -v -A -a4 -O2)



* Borland C++ 5.0 (options: -Oi -6 -v -A -a4 -O2)

** MS Visual C++ 6.0 (options: /G6 /Ox)

*** DJGPP 2.01 using pgcc 2.90.23 (options: -O6 -mcpu=pentiumpro -pedantic -fomit-frame-pointer)



* Borland C++ 5.0 (options: -Oi -6 -v -A -a4 -O2)

** MS Visual C++ 6.0 (options: /G6 /Ox)

*** DJGPP 2.01 using pgcc 2.90.23 (options: -O6 -mcpu=pentiumpro -pedantic -fomit-frame-pointer)