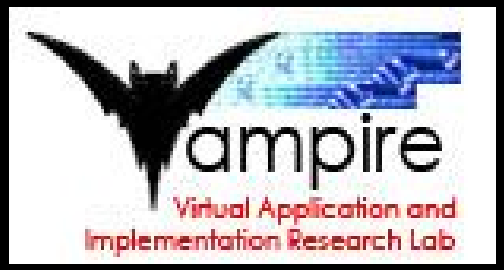

eBATS
CAINE
HOLMES
OLDMAN
and
FREEMAN
BEGINS
JUNE 17



Which public-key systems are best?

eBATS (ECRYPT Benchmarking of Asymmetric Systems) measures

- key-generation time,
- secret-key size,
- public-key size,
- encryption time,
- encrypted-message size,
- etc.

BATMAN

Measurements are carried out by BATMAN (Benchmarking of Asymmetric Tools on Multiple Architectures, Non-Interactively).

You can download BATMAN to reproduce results.

www.ecrypt.eu.org/ebats

Example measured on a Pentium 4 f12:

	sflashv2-1	ronald-3 2048
key-gen cycles	462090336	2467681772
secret-key bytes	2823	2048
public-key bytes	19266	256
sign cycles	1908060	63607084
sign 29 bytes	66	256
sign 709 bytes	746	752
verify cycles	667684	575108

Results show which systems are faster.

Example measured on a Pentium 4 f12:

cycles	implementation
29646848	claus-1 (using OpenSSL)
21324260	claus++-1 (using NTL)
13919316	claus++-1 (using GMP)

Results show which implementations are faster.

Note to implementers: GMP is very fast!

claus++-1 measured on different machines:

cycles	CPU
28981828	Intel Pentium 1 52c
27069568	Motorola PowerPC G4
13919316	Intel Pentium 4 f12
11306413	Sun UltraSPARC IV
9892179	AMD Athlon 622
3273274	AMD Athlon 64 X2 fb1
3082045	DEC Alpha 21264 EV6

Results show which computers are faster.

Want to advertise your system/implementation?

- Take a few minutes to turn your software into a BAT (Benchmarkable Asymmetric Tool) and submit it to eBATS.
- Measurements are continuing.
- Major reports in December 2006, July 2007.
- Intermediate announcements on web pages.

www.ecrypt.eu.org/ebats

Submit your BAT


NOW!
eBATS begins