Users of public-key cryptography have a choice of public-key cryptosystems, including RSA, DSA, ECDSA, and many more. Exactly how fast are these systems? How do the speeds vary among Pentium, PowerPC, etc.? How much network bandwidth do the systems consume?

The eBATS (CRYPTO Benchmarking of Asymmetric Systems) aims to answer these questions. The eBATS competition will identify the most efficient public-key systems among the submitted BATs (Benchmarkable Asymmetric Tools). Please submit your BAT according to the following API.

**Encrypted BAT** supports the following three functions:
- `keypair` returning a secret key and a public key;
- `ciphertext` reading a message and a public key, returning an encrypted message;
- `plaintext` reading an encrypted message and a secret key, returning the message that was encrypted.

**Signing BAT** supports the following three functions:
- `keypair` returning a secret key and a public key;
- `signedmessage` reading a message and a secret key, returning a signed message;
- `messagesigned` verifying a signed message and a public key, returning the message that was signed.

**Secret sharing BAT** supports the following three functions:
- `keypair` returning a secret key and a public key;
- `sharesecret` reading a secret key and another public key, returning a shared secret.

**Results**

BATMAN’s results on timings (generate a key, encryption, signing or secret sharing) and sizes (lengths of the keys, length of the ciphertext or signature) are stored in a huge database.

**CAVE** (Comparison and Visualization Environment) allows users to dynamically explore various graphs of BATMAN output, sliding between selected slices and projections of the database.

For more details on the API and to download BATMAN and CAVE visit [http://www.ecrypt.eu.org/ebats/](http://www.ecrypt.eu.org/ebats/).