



FOR IMMEDIATE RELEASE
February 27, 2003

Bart Preneel
Bart.Preneel@esat.kuleuven.ac.be
+32 (0)16 32 10 50

NESSIE PROJECT ANNOUNCES FINAL SELECTION OF CRYPTO ALGORITHMS

An open competition for the crypto algorithms of the 21st century.

The NESSIE project (New European Schemes for Signatures, Integrity and Encryption) (2000-2003) evaluates crypto algorithms. Crypto algorithms are the equivalent of locks, seals, security stamps and identification documents on the Internet. They are essential to protect our on-line bank transactions, credit cards, and personal information and to support e-commerce and e-government. Today, the NESSIE project announces the selection of a strong portfolio of crypto algorithms that will protect the information society.

In September 2000, cryptographers from more than 10 different countries all over the globe submitted 42 crypto algorithms. Since then, researchers inside and outside the NESSIE project have tried to attack these algorithms, attempting to find weaknesses that would compromise their security. In addition, the efficiency of these algorithms (how fast are they?) has been assessed. As a consequence of this evaluation, the set of 42 contenders has been reduced to 24 candidates in September 2001. A second selection phase ending today has reduced this number to 12; in addition, NESSIE recommends 5 algorithms that have been selected from existing or emerging standards.

Crypto algorithms are mathematical formulas that are essential to protect electronic information. They come in different flavours. Encryption algorithms are essential to protect sensitive information such as medical data, financial information and Personal Identification Numbers (PINs) from prying eyes. The project distinguishes between three types of encryption algorithms: block ciphers, stream ciphers and public-key encryption algorithms. Digital signature algorithms (in combination with hash functions) replace manual signatures in electronic transactions. A similar role can be played by MAC algorithms. Identification protocols allow to securely verify the identity of the party at the other end of the line.

Standards play an important role in the choice of a cryptographic algorithm. The NESSIE project is not a standardisation body (it does not write NESSIE standards), but the NESSIE project forms

the bridge between the research community and the user community by testing and comparing algorithms before standardising them. The NESSIE project intends to input these algorithms to standardisation bodies such as ISO (International Organisation for Standardisation) and the IETF (Internet Engineering Task Force).

NESSIE has selected the following 12 algorithms from the 42 submissions; in addition, 5 well established standard algorithms have been added to the NESSIE portfolio (indicated with a *):

Block ciphers:

- **MISTY1**: Mitsubishi Electric Corp., Japan;
- **Camellia**: Nippon Telegraph and Telephone Corp., Japan and Mitsubishi Electric Corp., Japan;
- **SHACAL-2**: Gemplus, France;
- **AES (Advanced Encryption Standard)* (USA FIPS 197) (Rijndael)**.

Public-key encryption:

- **ACE Encrypt**: IBM Zurich Research Laboratory, Switzerland;
- **PSEC-KEM**: Nippon Telegraph and Telephone Corp., Japan;
- **RSA-KEM* (draft of ISO/IEC 18033-2)**.

MAC algorithms and hash functions:

- **Two-Track-MAC**: K.U.Leuven, Belgium and debis AG, Germany;
- **UMAC**: Intel Corp., USA, Univ. of Nevada at Reno, USA, IBM Research Laboratory, USA, Technion, Israel and Univ. of California at Davis, USA;
- **CBC-MAC* (ISO/IEC 9797-1)**;
- **HMAC* (ISO/IEC 9797-1)**;
- **Whirlpool**: Scopus Tecnologia S.A., Brazil and K.U.Leuven, Belgium;
- **SHA-256*, SHA-384* and SHA-512* (USA FIPS 180-2)**.

Digital signature algorithms:

- **ECDSA**: Certicom Corp., USA and Certicom Corp., Canada;
- **RSA-PSS**: RSA Laboratories, USA;
- **SFLASH**: Schlumberger, France.

Identification schemes:

- **GPS**: Ecole Normale Supérieure, Paris, France Télécom and La Poste, France.

No weaknesses have been identified in any of these 17 algorithms. We believe that many of these algorithms present a significant improvement in the state of the art.

The 10 symmetric primitives in this portfolio (4 block ciphers, 4 MAC algorithms and 2 hash functions) can be used for free. The asymmetric primitives RSA-KEM, RSA-PSS and SFLASH are also in the public domain. PSEC-KEM is available under very favourable conditions. Licenses need to be negotiated for ACE Encrypt, ECDSA and GPS, but the owners have promised to offer reasonable and non-discriminatory terms.

It is quite remarkable that none of the six submitted stream ciphers meets the rather stringent security requirements put forward by NESSIE.

The evaluation process has been a fully *open* process based on published evaluation criteria. A significant effort has been spent by the project team. In addition, feedback has been received from the global cryptographic community; all comments have been made public. The project has interacted with a project industry board, which consists of representatives from the key European security vendors and users. Four well attended open workshops have been held to discuss the candidates and the evaluation results: November 2000 in Leuven (B), September 2001 in Egham (UK), November 2002 in Munich (D) and February 2003 in Lund (S).

Detailed evaluation reports on security and performance, as well as a document motivating the final selection are available at <http://www.cryptonessie.org>.

The NESSIE project is currently writing a specification of these algorithms which is targeted towards implementers and standardisation bodies. NESSIE encourages the community at large to include the algorithms in the NESSIE portfolio in standards and products.

NESSIE is a research project within the Information Societies Technology (IST) Programme of the European Commission (IST-1999-12324). The project partners are:

- Katholieke Universiteit Leuven (Belgium), coordinator;
- Ecole Normale Supérieure (France);
- Royal Holloway, University of London (U.K.);
- Siemens Aktiengesellschaft (Germany);
- Technion – Israel Institute of Technology (Israel);
- Université catholique de Louvain (Belgium);
- Universitetet i Bergen (Norway).

For more information about NESSIE, see our web site <http://www.cryptonessie.org>.