Submission to NESSIE

1. Name of submitted algorithms: **ACE Encrypt** and **ACE Sign**.

   Note: Because it is technically appropriate, we are submitting these two algorithms as a single submission. Nevertheless, it should be easy to evaluate the two algorithms independently.

2. Type of submitted algorithm, proposed security level, and proposed environment:

   Ace Encrypt: asymmetric encryption algorithm, secure against adaptive chosen ciphertext attack.

   Ace Sign: digital signature scheme, secure against adaptive chosen message attack.

3. Principal submitter's name, telephone, fax, organization, postal address, e-mail address:

   Victor Shoup
   IBM Zurich Research Laboratory
   Saeumerstrasse 4
   CH-8803 Rueschlikon/Switzerland
   Tel. +41-1-724-89-09 Fax. +41-1-724-89-53
   sho@zurich.ibm.com

4. Name(s) of auxiliary submitter(s): none

5. Name of algorithm inventor(s)/developer(s): Victor Shoup, Ronald Cramer

6. Name of owner, if any, of the algorithm (normally expected to be the same as the submitter): IBM and Ronald Cramer

7. Signature of submitter