

## Test Vectors for ACE Encrypt

Test vectors are supplied in the accompanying directory `tv`. The contents of these files are sequences of bytes, and in general, are not printable.

The files containing the public and private keys are as follows.

For  $a \in \{1024, 1280, 1536, 1792, 2048\}$ , and for  $b \in \{0, 1, 2, 3\}$ , the files named `epr.a.b` and `epu.a.b` contain the private and public keys, respectively, for a key instance with an  $a$ -bit modulus (i.e.,  $a$  is the security parameter input to the key generation algorithm).

The files containing sample cleartexts (inputs to encryption) are as follows.

- `i.1` – the empty message
- `i.2` – the message `"hello_world\n"`
- `i.3` – 1024 `a`'s (no newline)
- `i.4` – 1050 `a`'s (no newline)

Finally, the files containing the sample ciphertexts are as follows.

For  $a \in \{1024, 1280, 1536, 1792, 2048\}$ , and for  $b \in \{0, 1, 2, 3\}$ , for  $c \in \{1, 2, 3, 4\}$ , and for  $d \in \{0, 1, 2, 3, 4\}$ , the file `ct.a.b.c.d` contains an encryption of the message `i.c.d` under the public key `epu.a.b`. Also, the file `rv.a.b.c.d` contains the value of the secret exponent  $r$  used to generate the ciphertext; this number is written in standard hex notation.