NAME

rskeygen − generate private key pairs for TI graphing calculators

SYNOPSIS

rskeygen [**--secure**] [**--ti**] [**--length** *nbytes*]

DESCRIPTION

rskeygen generates application and OS signing keys for the Texas Instruments TI-73, TI-83 Plus, TI-84 Plus, TI-89, and TI-92 Plus graphing calculators. These keys consist of two prime numbers *p* and *q* as well as their product *n*. Current calculator models impose a limit of 512 bits (64 bytes) on the size of *n*, so *p* and *q* are generally about 256 bits each. As of this writing this means factoring *n* is beyond the reach of most people, though this will undoubtedly change in the future.

The keys generated by **rskeygen** are not very useful at the moment, because in order for an application or OS to be accepted by the calculator, the key used to sign it must itself be signed using the calculator's own (possibly unique) private key, which is only known to TI. Nevertheless, **rskeygen** is provided in the hope that it can be useful, both for testing and for devising new signature schemes based on TI's.

OPTIONS

--secure

Attempt to generate a ‘‘secure’’ key using the system's entropy pool, /dev/random (see **random**(4).) The actual security is thus dependent on your system's implementation of /dev/random.

Without **--secure**, the keys are generated based on the current time and process ID, which is not secure in the slightest.

--ti

Generate keys which are palatable to TI's official app signing programs. This forces *p* to be congruent to 3 and *q* to 7 modulo 8. This option is not necessary when using **rabbitsign**(1), nor is it necessary for the calculator to validate signatures properly.

--length *nbytes*

Specify the length in bytes of the modulus *n*; *p* and *q* are each calculated to be approximately half this length. This should not be greater than 64 for current calculators, and must be less than 256 in any event due to a limitation of the key file format.

SEE ALSO

rabbitsign(1), **packxxk**(1)

AUTHOR

Benjamin Moody <floppusmaximus@users.sf.net>