RSA Cryptosystem

Petri Tuononen - Jukka Tuominen - Jani Kirsi

for educational use to teach cryptography

See every encryption/decryption phase that are done by the RSA cryptosystem.
Great way to teach and learn cryptography.

Assymmetric public key cryptosystem. Generates public and private keys.
Create encrypted messages.
Secure and popular.

Secure mode:

* Generate higly secure public and private keys automatically (user selectable bitsize).
* Save and load keys.
* Hide keys from view.
* Use public key to encrypt message (three types of padding schemes available).
* Use private key to decrypt message.

Teach/learn mode:

* User selectable primes and public key exponent.
* You can try to encypt the message on your own by using pen and paper. Then you can enter the primes and the public key exponent you selected to the program and it prints all stages that are done by the RSA cryptosystem with given padding scheme.
* Three padding schemes to choose from. It is even possible to display all three paddings scheme types vertically when encrypting/decrypting.
* Save/load encryption/decryption execution lines.
* Show/hide public/private key exponent.
* Show execution lines on full screen (separate window).

ICT-Showroom 5.3.2009 11-15