TECP – Tutorial Environment for Cryptographic Protocols

Jelena Zaitseva

Institute of Computer Science, University of Tartu
Why?

- Cryptography is taught and studied at universities.
- There is almost no educational software for such courses covering public key cryptography.
Problem Formulation 1

Tutorial environment must

- enable visualization of protocols, including values of secret parameters and intermediate results (all values can be arbitrary large),
- allow adding/removing communicating parties,
- allow adding/editing/sending/removing arbitrary parameters,
- handle number-theoretic and cryptographic primitives
Problem Formulation 2

Analyzed protocols:
- Diffie-Hellman key exchange algorithm
- RSA signatures and encryption schemes
- Rabin public key encryption scheme
- ElGamal signature and encryption schemes
- DSA
- Chaum’s blind signature scheme
Problem Formulation 3

Required mathematical operations:

- calculation
  - $a \mod b$, $a - b$, $a + b$, $a \cdot b$, $a/b$, $a^b$,
  - $a^b \mod n$ ($-1$ can also be a value of $b$),
  - $\gcd(a, b)$,
  - hash value of $m$,

- generation and verification
  - prime numbers,
  - number from $\mathbb{Z}_n$ ($\mathbb{Z}_n^*$),
  - generator of $\mathbb{Z}_n^*$
  - number congruent to $a \mod b$,

where $a$, $b$, $n$ and $m$ are some positive integers.
Overview of TECP
Implementation

- Borland ®Kylix™ 3 Open Edition, Borland ®Delphi™ 6 Personal Edition
- FGInt
- TParser 10.1
Conclusion

TECP can be used in the following ways:

- visual aid
- tool for experimenting with protocols
- modular arithmetic operations calculator
- problem generator
Thank You for Your attention!