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

K –н теср			
Eile Edit View Help	🕅 All Values		• ×
D 🚅 🖬 🗠 🗠 🞯 👩 f(x) 🗡	- 🗇 Bin	🔎 Dec	🗇 Hex
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	Alice p=53713936060 alpha=8731953 a=81789621205 beta=81006453i k=17551676393 r=27117234518 m=28141022664 942136415762782 h=13731904006 s=29658912163 Bob p=53713936060 alpha=8731959; beta=81006453i r=27117234518 m=28141022664 s=29658912163 V=1054118965 V=1054118965 Eve p=53713936060 alpha=8731959; beta=81006453i r=27117234518 m=28141022664 s=29658912163	12477525125655043677 34737642764528657532 3489790876329862839 35114119274013032070 7699235364765350875 93975978039955203026 16305939559411818036 81056255413159907490 14886857550603504952 2217987533716082839 34737642764528657532 35114119274013032070 93975978039955203026 16305939559411818036 2217987533716082839 3195683259760086261 3195683259760086261 3195683259760086261 3195683259760086261 3195683259760086261 3195683259760086261 3195683259760086261 3195683259760086261 3195683259760086261 3195683259760086261 3195683259760086261 3195683259760086261 32477525125655043677 34737642764528657532 35114119274013032070 93975978039955203026 16305939559411818036 2217987533716082839 16305939559411818036 2217987533716082839 16305939559411818036 2217987533716082839 16305939559411818036 2217987533716082839 16305939559411818036 2217987533716082839 16305939559411818036 2217987533716082839 16305939559411818036 2217987533716082839 16305939559411818036 2217987533716082839 16305939559411818036 2217987533716082839 16305939559411818036 2217987533716082839 16305939559411818036 2217987533716082839 16305939559411818036 2217987533716082839 16305939559411818036 2217987533716082839 16305939559411818036 2217987533716082839 16305939559411818036 2217987533716082839 16305939559411818036 2217987533716082839 16305939559411818036 2217987533716082839 16305939559418 16305939559418 16305939559418 16305939559418 16305939559418 16305939559418 16305939559418 1630594 163059	356597740672426915294; 89466 076454520437658546208(9581975714862354810087 54335 358280160453657505734 5285686586 07689011860478203 15285686586 158096722986500217 530685558799368787347; 356597740672426915294; 35686586 530685558799368787347; 841051368650017005988; 841051368650017005988; 841051368650017005988; 356597740672426915294; 89466 1581975714862354810087 3358280160453657505734 5285686586 530685558799368787347; 356597740672426915294; 841051368650017005988; 841051368650017005988; 356597740672426915294; 289466 1581975714862354810087 3358280160453657505734 5285686586 530685558799368787347;

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 experementing with protocols
- modular arithmetic operations calculator
- problem generator

Thank You for Your attention!