Distributed Lab

Certificate

This certifies that

TOPICS

Basic properties and Coding of information • Cryptology • Basic definitions (plaintext, ciphertext, key, algorithm, protocol) • Modular arithmetic. Group, field • Hash functions. SHA • Symmetric encryption. The structure of the modern encryption methods. DES/AES • Caesar cipher. Vigenère cipher • Statistical analysis • Key exchange protocols • Key transfer problem • Absolutely stable cryptosystem • Key exchange. Diffie-Hellman protocol • Asymmetric encryption algorithms. RSA • Public key infrastructure • Digital signatures • RSA Digital Signature Verification • Elliptic curve mathematic • Elliptic curves • Group of points of an elliptic curve • Elliptic curve point group arithmetic • Digital signatures in cryptocurrencies • Blind digital signatures, Ring digital signatures • Security problems in cryptosystems • Threats of cryptosystems

Pavel Kravchenko, PhD
CEO & founder Distributed Lab

Oleksandr Kurbatov
Researcher at Distributed Lab

Bohdan Skriabin
Researcher at Distributed Lab