How to extract the plaintext without knowing the secret key while following NIST or ISO/IEC recommendations for modes of operations of block ciphers

RAMP SESSION

FSE08

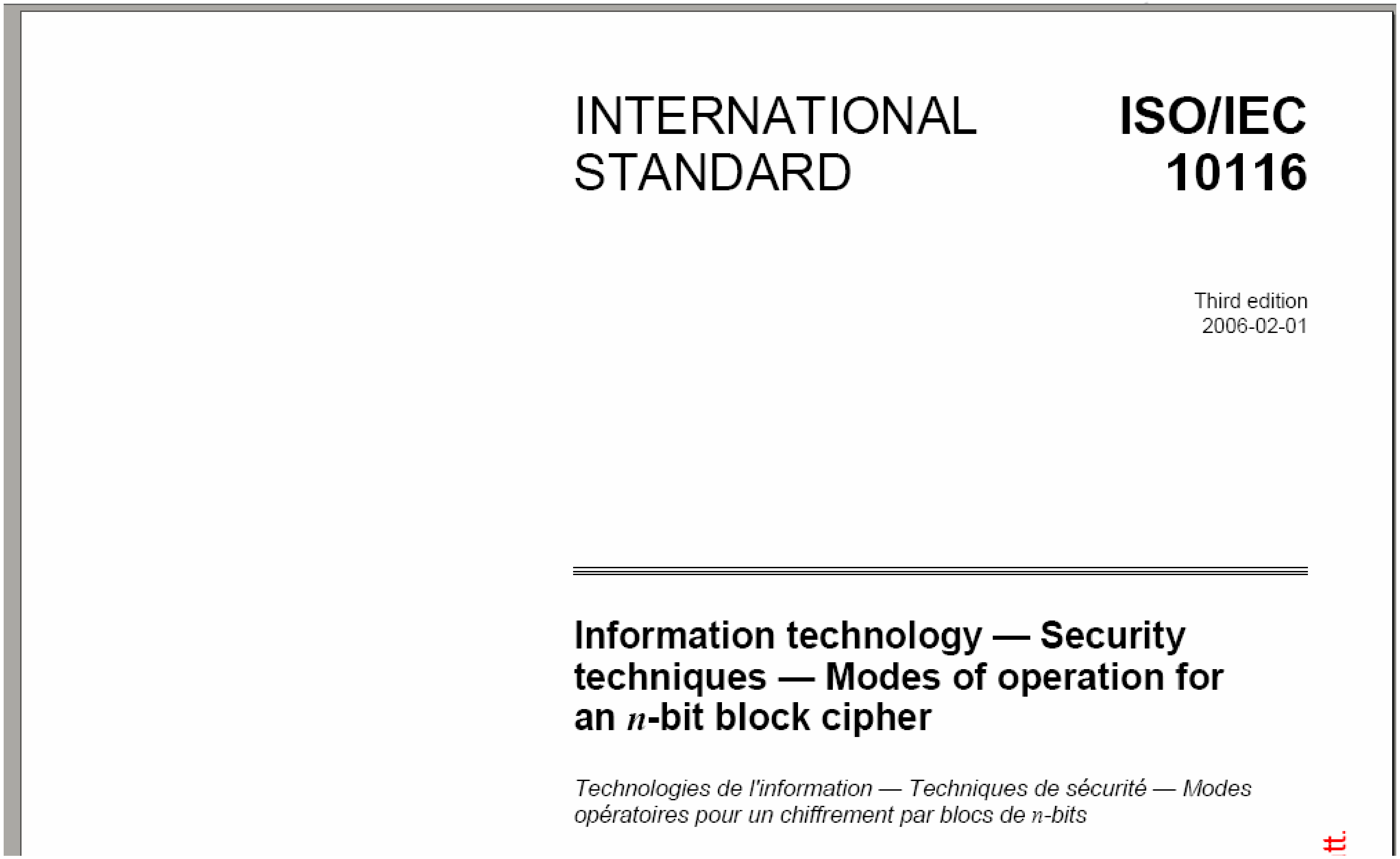
Speaker Danilo Gligoroski

Centre for Quantifiable Quality of Service in Communication Systems,

NTNU

The key separation principle for different modes of operation of the block ciphers is a cryptographic folklore wisdom that states:

One should always use distinct keys for distinct algorithms and distinct modes of operation.



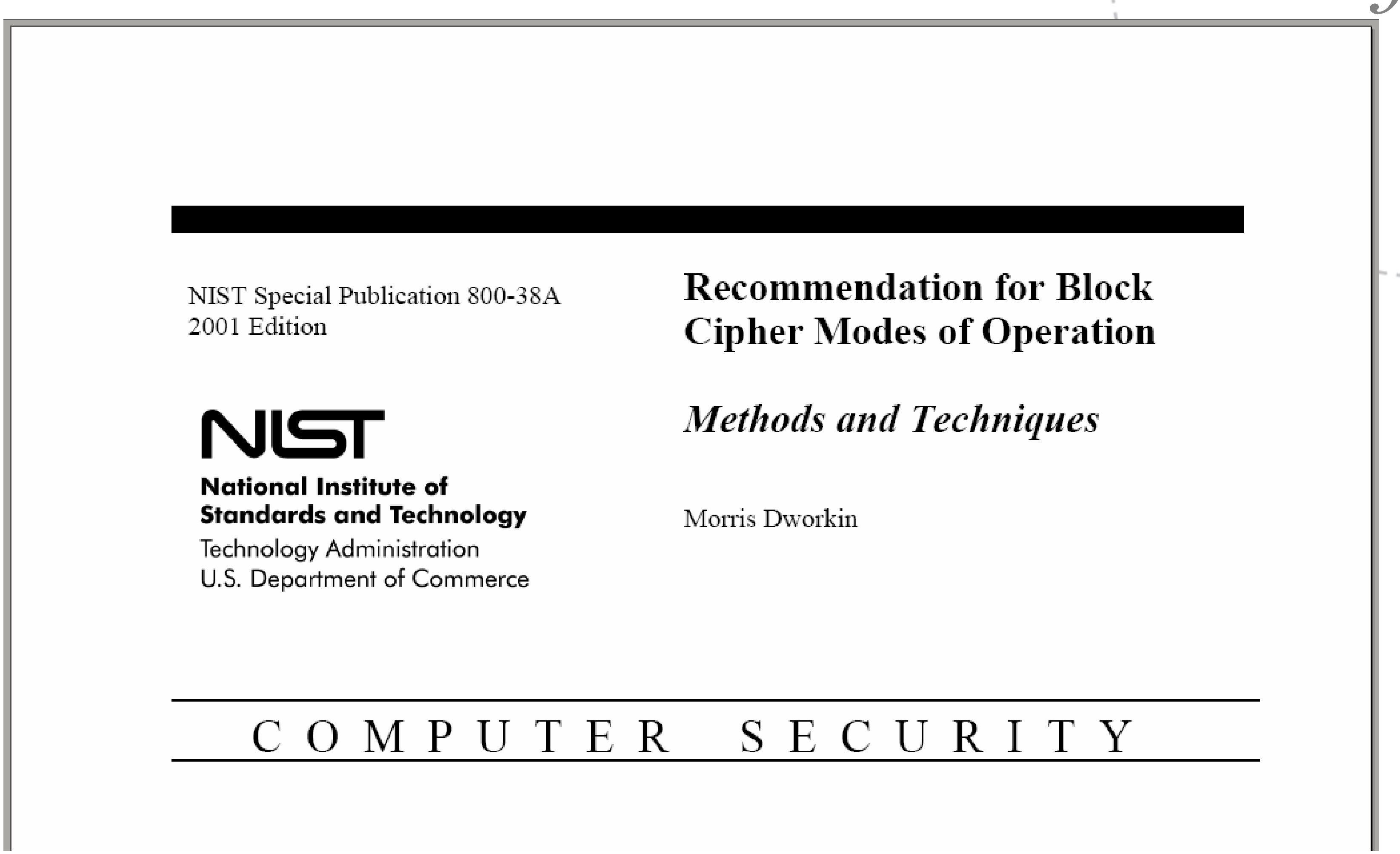
INTERNATIONAL STANDARD

ISO/IEC 10116

Third edition
2006-02-01

Information technology — Security techniques — Modes of operation for an n-bit block cipher

Technologies de l'information — Techniques de sécurité — Modes opératoires pour un chiffrement par blocs de n-bits



NIST Special Publication 800-38A
2001 Edition

Recommendation for Block Cipher Modes of Operation

Methods and Techniques

Morris Dworkin

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

COMPUTER SECURITY

- NIST Special Publication 800-21 2005, *“Guideline for Implementing Cryptography In the Federal Government”* and NIST Special Publication 800-57 2007, “Recommendation for Key Management Part 1: General (Revised)”
- *“Keys used for one purpose shall not be used for other purposes.”*
- *“In general, a single key should be used for only one purpose (e.g., encryption, authentication, key wrapping, random number generation, or digital signatures)”.*
- *“Some uses of keys interfere with each other”, but the interference is explained only by interchangeable use of one key for key transport and digital signatures.*

- In ISO/IEC 10116 standard there is just a brief mentioning that: *"How keys and starting variables are managed and distributed is outside the scope of this International Standard".*
- However!!!!
- **All examples that explain different modes of operation use a same encryption key??!?!**

```
• vi OnceUponATimeInTheWest.txt
• dd if=/dev/zero of=zero.txt bs=4096 count=1024
• openssl enc -aes-128-cbc -in zero.txt -out zero.bin -K
  01234567890123456789012345678901 -iv
  0123456789abcdef0123456789abcdef – nopad
• openssl enc -aes-128-ofb -in OnceUponATimeInTheWest.txt –out
  EncryptedDoc.bin -K 01234567890123456789012345678901 -iv
  0123456789abcdef0123456789abcdef  -nopad
• vi EncryptedDoc.bin
• ./XORFiles zero.bin EncryptedDoc.bin Extracted.txt
• vi Extracted.txt
```