

---

# Influence of US Cryptography (Developments&Regulations) on Russian Cryptography

Anatoly Lebedev

President

LAN Crypto, Ltd

# Some History

---

- ◆ 1952 - NSA created  
( *and the author born*)
- ◆ 1960 - Martin & Mitchell case
- ◆ 1963 - Dunlap and Hamilton cases
- ◆ 1967 - D. Kahn “The Codebreakers”  
published

# Cryptography Going Public

---

- ◆ 1973 - First Draft of DES
- ◆ 1976 - W. Diffie and M. Hellman paper
- ◆ 1977 - RSA public-key method invented

# Cryptography Going Public

---

- ◆ 1977 - DES issued as a FIPS
- ◆ 1978-1979 - new cryptographic schemes by  
G. Davida, R. McEliece,  
M. Rabin, H. Williams,  
Merkle-Hellman,  
Pohlig-Hellman, etc.,  
published

# Cryptography Going Public

---

- ◆ W. Diffie, M. Hellman, R. Merkle,
- ◆ R. Rivest, A. Shamir, L. Adleman,
- ◆ R. McEliece, M. Rabin, G. Simmons,
- ◆ G. Davida, D. Denning, J. Massey etc..



# US: The First “Cold Wave”

---

- ◆ 1979 - B. Inman’s speech  
American Council on Education,  
Study Group (PCSG) created
- ◆ 1981 - PCSG Report: two-year experiment  
of NSA prepublication review
- ◆ 1984 - National Security Decision Directive  
( NSDD-145, September, 1984)

# USSR :Just “a Little Colder”

---

- ◆ 1985 - publicly available textbook  
in cryptography by A. Konheim  
“CRYPTOGRAPHY: A Primer” ,  
NY, John Wiley & Sons, 1981
- ◆ translated,
- ◆ confiscated,
- ◆ classified



# US: “Back Office” Still Works

---

- ◆ Patents of that Time
- ◆ 1980 - Diffie-Hellman Key Exchange  
(1977) US Patent # 4,200,770
- ◆ 1980 - Merkle-Hellman Knapsacks  
(1977) US Patent # 4,218,582

# “Back Office” (Continued)

---

- ◆ 1983 - RSA  
(1977) US Patent #4,405,829
- ◆ 1984 - Pohlig-Hellman,  
US Patent #4,424,414

# Almost the Same Game

---

- ◆ 1986 - \*. \*\*\*\*\*\*, \*. \*\*\*\*\*\*, A. Lebedev,  
(1980) \*. \*\*\*\*\*\*, \*, \*. \*\*\*\*\*\*,  
USSR Patent # 244,375
- ◆ 1987 - A. Lebedev, \*. \*\*\*\*\*\*,  
(1980) USSR Patent # 251,378
- ◆ 1987 - , A. Lebedev, \*. \*\*\*\*\*\*,  
(1985)   
USSR Patent # 251,387

# STU- III

---

- ◆ August 1983 - 50-person NSA Task Force  
headed by N. Piazzola  
created by W. Deely
- ◆ October 1983 - AT&T Bell Labs  
reported back OK
- ◆ April 1984 - five corporations selected  
AT&T, GTE, ITT,  
Motorola, RCA

# STU-III (Continued)

---

- ◆ November 1984 - The studies completed  
Competition to chose three
- ◆ March 1985 - AT&T, Motorola, RCA  
selected
- ◆ April 1986 - Schedule to deliver prototypes
- ◆ Late 1986 - The end of the field evaluation
- ◆ April 1987 - First production

# CYLINK Corp.

---

- ◆ 1985 - CY512, CY1024

Digital Exponentiation Processors  
designed and manufactured

- ◆ 1024bits-Exponentiation

Made as Fast as  
0.3 sec.

# USSR: “To Do or Not to Do”

---

- ◆ 1987 - Some First Reviews of Possibilities  
and Plans
- ◆ 1988 - Resolution “To Do”
- ◆ 1993 - Estimated Time to Get Some  
Practical Results

# US: “Wave Back”

---

- ◆ 1987 - Computer Security Act (CSA)
- ◆ 1992 - Freedom of Information Act  
litigation by CPSR
- ◆ 1992 - Electronic Frontier Foundation  
opposing the FBI proposal



# USSR: “Storm Back”

---

- ◆ 1991- August, 19 GKChP-coup
- ◆ 23 Russia started
- ◆ 29 Cryptography and Gov. Communications out of KGB
- ◆ New Gov. Communications Committee ( KPS) under President M. Gorbachev

# Storm Back (Continued)

---

- ◆ 1991 - December, 9 the corporation “LAN Crypto” founded
- ◆ 1991 - December, 21 USSR finished
- ◆ 1993 - January, New Russian Standards for Digital Signature&Hash, Message Encryption, Key Generation
- ◆ proposed by “LAN Crypto”

# Proposed Standards

---

- ◆ Athena - Key Generation Method based on Diffie-Hellman-like algorithm, but different one-way functions
- ◆ Vesta - Stream Cipher (Software Oriented) Method to Encrypt Electronic Messages

# Proposed Standards (Continued)

---

- ◆ Notary - Digital Signature Method based on ElGamal-like algorithm, but different one-way functions
- ◆ Hera - Hash Algorithm based on linear shift registers over finite rings

# Russian Government Initiatives

---

- ◆ 1993 - March, Gov. Com. Commit.(KPS) renamed as Federal Agency for Govern. Communications and Information under the President of RF (FAPSI) - March, New Law on FAPSI
- ◆ 1993 - March, New Law on FAPSI issued
- ◆ 1993 - March, LAN Crypto proposals were opposed by FAPSI

# FAPSI “Initiatives”

---

- ◆ 1993 - May, FAPSI Letter to Russian Central Bank
- ◆ 1993 - June, LAN Crypto - FAPSI agreement on certification
- ◆ 1994 - January, Rejection to accept the “Vesta” and “Notary” algorithms as “FAPSI recommended”

# US Government Initiatives

---

- ◆ 1991- August, The DSS Draft Presentation  
before The US Congress
- ◆ 1993 - April , The Key-Escrow Initiative  
“Clipper” chip
- ◆ 1994 - May, 19 DSS Adopted as a National  
Digital Signature Standard

# Russia:FAPSI Initiatives

---

- ◆ 1994 - April, 27 FAPSI and GTK\*  
Regulation on Information  
Security Business

---

\*) State Technical Commission

- ◆ 1994 - May, 24 FAPSI-designed Russian  
Digital Signature Standard  
GOST 34.10 Published  
(Adopted on Jan.1, 1995)



# FAPSI Initiatives (Continued)

---

◆ 1994 - Dec., 24 Gov. Resolution #1418

“On Licensing . . .”

Adopted

◆ 1995 - April, 3 Presidential Decree #334  
on “encryption means”

# US: Some New Bills

---

- ◆ 1996 - February, “Security and Freedom Through Encryption (SAFE) Act” .
- ◆ 1996 - March, “Encrypted Communications Privacy Act of 1996” . (S.1587)
- ◆ 1996 - March, “Promotion of Commerce On-Line in the Digital Era (Pro-CODE) Act 1996” .

# New Bills ( Continued)

---

- ◆ 1996 - July, US Congress Pro-CODE Hearings
- ◆ 1996 - October 1, The Vice-President 1996 - October 1, The Vice-Statement
- ◆ 1996 - October 2, Key Recovery Alliance

# “New Initiatives”

---

- ◆ 1996 - Aug. 12, LAN Crypto v FAPSI  
Moscow Arbitration Ct.
- ◆ 1996 - Oct. 3, Appelation rejected
- ◆ 1996 - Sept. 2, FAPSI v Signal-COM  
Moscow Arbitration Ct.
- ◆ 1996 - Nov. 4, Appelation rejected

# Russia: Licensing Bills

---

- ◆ 1996 - October, The Final Draft of the Federal Law “On Licensing”  
Adopted by Duma
- ◆ 1996 - November, New Presidential Decree #1268 “On Regulation of dual-purpose technologies export” Made actual