HISTORY OF CRYPTOGRAPHY

presented by Nikita Borisov
Classic Ciphers

- Thousands of years old
- Caesar cipher
  - ABCDEFG… => DEFGHI...
  - Rot13
- Substitution ciphers
  - ABCDEFG… => IWNTPOM...
  - Newspaper cryptograms
- Polyalphabetic ciphers
Pre-WWII Cryptography

- Development of statistics for cryptanalysis
- Still pen & paper design
Most famously, Enigma machine
Automated encryption
Automated cryptanalysis
  “Bombe”
  First made in Poland
  Improved upon in the UK by a team including Alan Turing
1970’s: Open Cryptography

- Not just for spooks anymore
- 1975: Data Encryption Standard
  - Designed by IBM
  - Enhanced (?) by NSA
  - Analyzed by academics
- 1976: Public key cryptography
1980’s: Dam breaks open

- New primitives:
  - Oblivious transfer
  - Commitment
  - One-way functions
  - Zero-knowledge proofs
  - Secure multi-party computation

- New applications:
  - Games (poker)
  - E-cash
  - Voting
  - Anonymous communications
  - Contract signing
  - …
1990’s: Open Cryptography Catches Up

- DES finally understood
- … and broken
  - 1998 EFF, $250K
  - 2006 COPACOBANA, $10K
- AES competition held
  - Open design, analysis
  - No “advice” from NSA
- Many industrial algorithms broken
  - GSM, 802.11, etc.
1990’s: Cryptography Becomes Commonplace

- In email
  - PGP
  - S/MIME
- On the Internet
  - Kerberos
  - SSH
  - IPSec
- On the web
  - SET
  - SSL/TLS

- Standard protocols for:
  - Encryption
  - Authentication
  - Public key cryptography
  - Communications security

- What’s left?
2000’s: A New Beginning

- Moore’s Law: “fancy” schemes become practical
  - Encrypted computation
  - Anonymous credentials
  - Private information retrieval
- New primitives
  - Pairing-based cryptography
  - Identity-based cryptography
  - New homomorphisms
- New applications
  - Even smart cards can do public key crypto
  - New constraints, attacks (e.g., side channels)
Cryptography: Exciting again

\[ y^2 = x^3 - x \]

\[ y^2 = x^3 - x + 1 \]