

Cryptography Standards Evolution

Rudra Murthy CISO UIDAI-MSP

Agenda

- ▶ Encryption Norms in India
- ▶ Research Initiatives
- ▶ Current ongoing Research Areas in Cryptology

Encryption norms in India

- ▶ ISP license issued in 1998-99 by DoT limits the level of encryption by 40 bit key length and for the use of more than this prescribed limit, written permission from DoT is required with mandatory deposit of decryption key with DoT.
- ▶ The IT amendment Act passed in 2008 which has amended the IT Act of 2000, and has come into effect from 27th of Oct 2009, has led to addition of Section 84 A, which says that the Central govt may, for secure use of electronic medium and for promotion of e-Governance and e-commerce prescribe the modes or methods of encryption.
- ▶ Section 69 of IT Act 2000 empowers the, Central Government/State Government/ its authorized agency to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource if it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence or for investigation of any offence.

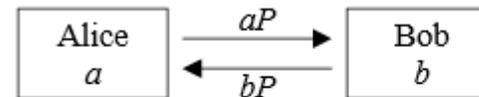
Research Initiatives

- ▶ Cryptology Research Group
- ▶ Cryptology Research Society of India
- ▶ DSCI
- ▶ The Institute of Mathematical Sciences (IMSc)

Ongoing Projects by Cryptology Research Group

- ▶ Strategic Japanese-Indian Co-operative Programme on "Multidisciplinary Research Field which combines Information and Communications Technology with Other Fields".
- ▶ "Research and development of some cryptographic primitives", funded by Department of Information Technology.
- ▶ "Research and Development of Bilinear Pairing Based Protocols", funded by Department of Information Technology.

It is easy to see that the DHP reduces in polynomial time to the DLP. It is generally assumed, and has been proven in some cases that the DLP(discrete logarithm problem) reduces in polynomial time to the DHP



- ▶ "Block Cipher", funded by Indian Space Research Organization. Two-party one-round key agreement protocol.
- ▶ "Implementation of Provably Secure Public Key Protocols", funded by Indian Statistical Institute

Ongoing Projects by Cryptology

- ▶ Symmetric Key Cryptography
 - ▶ Stream Cipher
 - ▶ Boolean Functions
- ▶ Public Key Cryptography
 - ▶ RSA Cryptosystem
 - ▶ Identity Based Encryption
 - ▶ Signcryption
 - ▶ Public Key Primitives
- ▶ Cryptographic Hash Functions
 - ▶ Modes of Operation
 - ▶ Compression Functions
 - ▶ Programmable Hash Functions
- ▶ Sensor Networks and Broadcast Cryptography
 - ▶ Key Predistribution
 - ▶ Combinatorial and Probabilistic Analysis
 - ▶ Authentication
- ▶ Coding Theory
 - ▶ Batch Codes
 - ▶ Locally Decodable Codes

Thanks You