Cybersecurity, Nuclear Security, Alan Turing, and Illogical Logic

A Turing Lecture by Martin E. Hellman

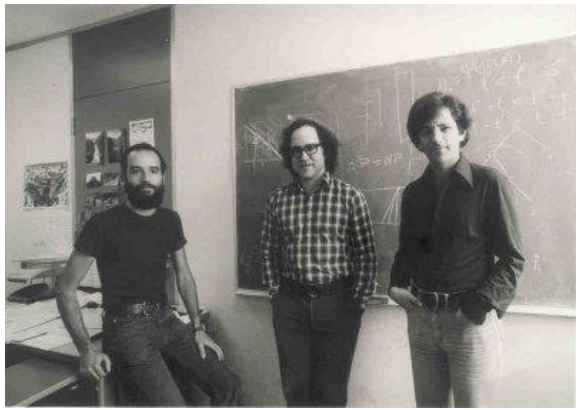
Presented by David Araújo for the Applied Cryptography course at University of Aveiro, December 2023

How it began...

- The National Institute of Standards and Technology (NIST) birthed a “defective” encryption standard, DES, inadequate from the start with a insufficiently large key.
- When technology and science must accommodate politics and the urge to project force to the exterior.

The Public Key Era

DES controversy and Public Key evolution

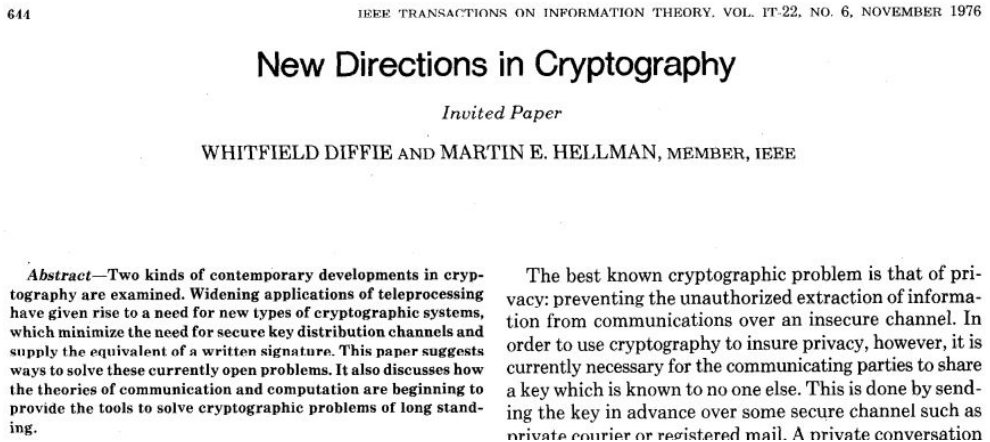


- DES keys were too large for NSA, used to using small keys which could be easily broken at a small cost.
- With public key cryptography, key could be changed as frequently as desired, driving the cost past reasonable limits for an attacker.
- From *trapdoor cryptosystems* (TDCs) to public keys and the unintended *trapdoors* in DES.
- *Merkle puzzles* and distribution puzzles.
- First working public key cryptosystem was not realized until RSA.

Born Classified

Of National Interest

- Hellman and Diffie decided to go public in exposing DES weakness.
- NSA and Stanford University legal dispute.
- Merkle and Pohlig reightfull recognition.
- *Crypto wars* first impact in policy took time.



New Directions in Cryptography

Invited Paper

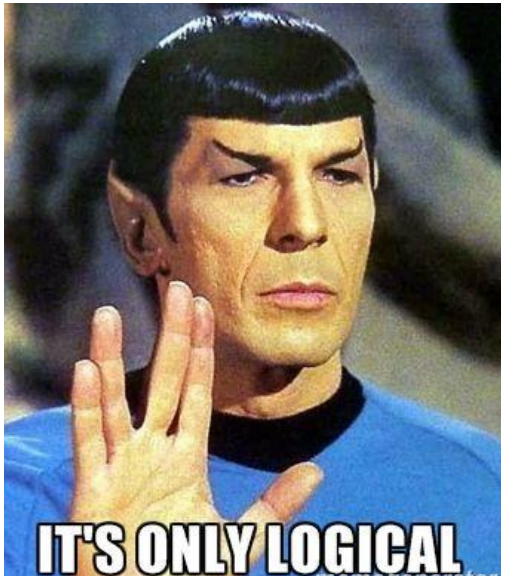
WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

***Abstract*—Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.**

The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such as private courier or registered mail. A private conversation

Cyber-deterrence

It's only logical



- Deterrence necessitates rationality from the adversary and irrationality from the one.
- Can when trust logic and irrationality to out leaders?
- RSA and Diffie-Hellman Key Exchange in a *post quantum* era.
- Logic is only one of the lenses to see the world