Cypherpunk History

Summer Sessions with
OC Bitcoin Network
6/29/23

Cypherpunks: Shadowy super-coders or nerds?

Ian Avrum Goldberg (2016). Cryptographer and cypherpunk. Best known for breaking Netscape's implementation of SSL and cracking 40-bit encryption.

Table of contents

Cold War encryption

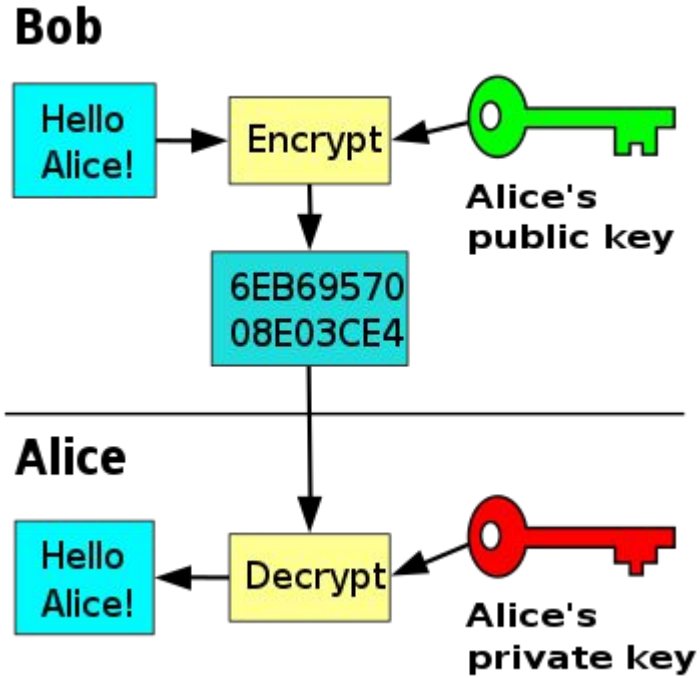
- World War 2 illustrated that code-breaking and cryptography can play an integral part in national security and the ability to prosecute war.
- In the early days of the Cold War, the U.S. and its allies developed an elaborate series of export control regulations designed to prevent a wide range of Western technology, including encryption, from falling into the hands of enemies

Business vs. government

- Encryption export controls became a matter of public concern with the introduction of the personal computer.
- Due to restrictions on encryption, businesses had to develop two versions of their software: The "U.S. version" which supported full size encryption of 128-bits or larger and the "International version" which was limited to 40-bits.
- Encryption the government could not break was considered a munition (aka weapon).

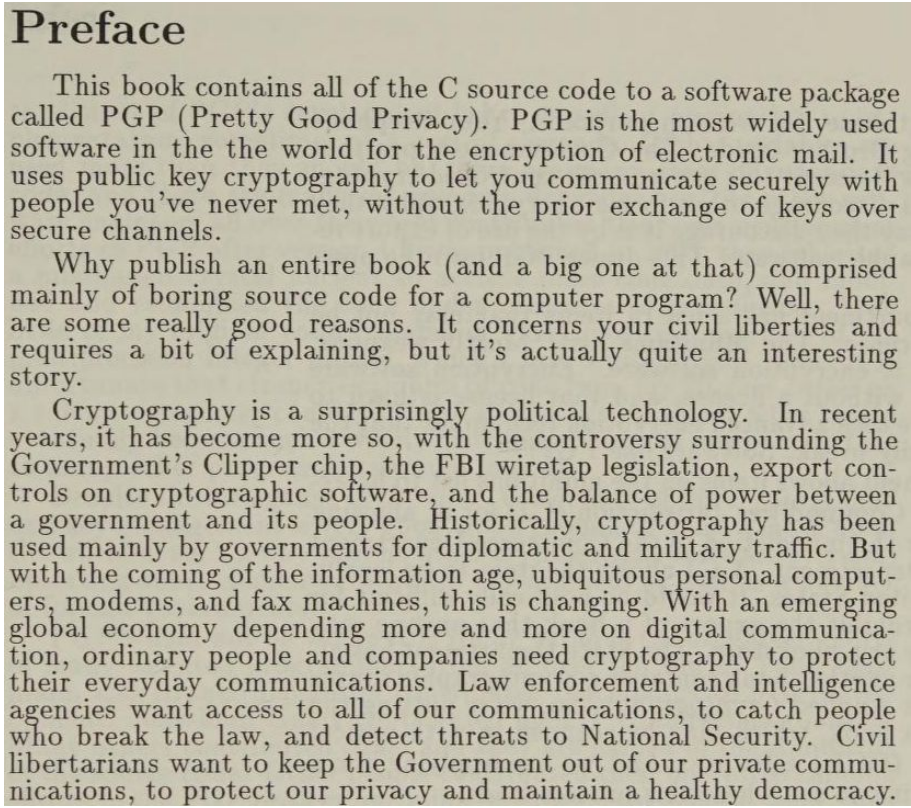
Public and private key cryptography

- RSA (Rivest–Shamir–Adleman; 1977) is a public-key cryptosystem, one of the oldest, that is widely used for secure data transmission.
- Messages can be encrypted by anyone, via the public key, but can only be decoded by someone who knows the prime numbers.



Pretty Good Privacy (PGP)

- Pretty Good Privacy (1991) is an encryption program that provides cryptographic privacy and authentication for data communication developed by Phil Zimmermann.
- No license fee was required for its non-commercial use, and the complete source code was included with all copies, subverting the government's restrictions on encryption.
- PGP found its way onto the Internet and was quickly adopted around the world.
- In February 1993, Zimmermann became the formal target of a criminal investigation by the US Government for "munitions export without a license." After several years, the investigation of Zimmermann was closed without filing criminal charges against him or anyone else.



Preface

This book contains all of the C source code to a software package called PGP (Pretty Good Privacy). PGP is the most widely used software in the the world for the encryption of electronic mail. It uses public key cryptography to let you communicate securely with people you've never met, without the prior exchange of keys over secure channels.

Why publish an entire book (and a big one at that) comprised mainly of boring source code for a computer program? Well, there are some really good reasons. It concerns your civil liberties and requires a bit of explaining, but it's actually quite an interesting story.

Cryptography is a surprisingly political technology. In recent years, it has become more so, with the controversy surrounding the Government's Clipper chip, the FBI wiretap legislation, export controls on cryptographic software, and the balance of power between a government and its people. Historically, cryptography has been used mainly by governments for diplomatic and military traffic. But with the coming of the information age, ubiquitous personal computers, modems, and fax machines, this is changing. With an emerging global economy depending more and more on digital communication, ordinary people and companies need cryptography to protect their everyday communications. Law enforcement and intelligence agencies want access to all of our communications, to catch people who break the law, and detect threats to National Security. Civil libertarians want to keep the Government out of our private communications, to protect our privacy and maintain a healthy democracy.

40-bit encryption broken

- On January 28th, 1997, RSA Data Security Inc. challenged the world to decipher a message encrypted using a 40-bit key, the longest keysize allowed for export. RSA offered a $1,000 reward, designed to stimulate research and practical experience.
- Goldberg decrypted the message in a mere 3.5 hours after the contest began, providing very strong evidence that 40-bit ciphers are totally unsuitable for practical security.
- Legal challenges and other civil libertarians and privacy advocates, led to a series of relaxations in US export controls, culminating in 1996 with Executive Order 13026, transferring commercial encryption from the Munition List to the Commerce Control List.


```
12 35 13 64 78 d3 da 08 d9 15 ed 20
89 30 5f 50 68 5c 6c b4 bf 5b 00 38
ff 44 4e d9 d4 9b 46 16 fb 12 92 62
9b d4 7f 1a 8d 48 fe b6 63 d1 d4 c2
eb 19 0d 86 3f f4 43 75 9a 58 06 2c
8b a5 9e 6a 33 30 c3 3e a8 ab 24 25
```

This is why you should use a longer key.

Wei Dai’s “b-money”

- In 1998, Dai helped to spark interest in cryptocurrencies with the publication of "b-money, an anonymous, distributed electronic cash system,” cited in the bitcoin whitepaper.
- In the paper, Dai outlines the basic properties of all modern day cryptocurrency systems: "a scheme for a group of untraceable digital pseudonyms to pay each other with money and to enforce contracts amongst themselves without outside help."

Adam Back’s “hashcash”

- Hashcash is a proof-of-work system used to limit E-mail spam and denial-of-service attacks. Hashcash was proposed in 1997 by Adam Back and described more formally in Back's 2002 paper "Hashcash - A Denial of Service Counter-Measure."
- Hashcash was an early precursor to digital cash. Satoshi cited it as his inspiration for the proof-of-work implementation in Bitcoin.

Satoshi Nakamoto’s “bitcoin”

- Double-spending is a fundamental flaw in a digital cash protocol in which the same single digital token can be spent more than once.
- Due to the nature of cyberspace, in comparison to physical space, a digital token (like a file) is inherently duplicable. Solutions to this problem required a central authority to determine ownership and transfer of the digital token.
- Prior attempts at digital cash were not sufficiently decentralized.
- Bitcoin implemented a solution in early 2009. Its cryptographic protocol used a proof-of-work consensus mechanism where transactions are batched into blocks and chained together using a linked list of hash pointers–the blockchain.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.