RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: BAS-M06

Crypto 101:
Encryption, Codebreaking, SSL and Bitcoin

Benjamin

HVF Labs

@BenjaminJun

HVF

Some material adapted from Ivan Ristic, Qualys (RSAC 2011)

Crypto 101

Cryptography is the art and science of keeping messages secure.

- Cryptography building blocks
- Cryptographic protocols
  - SSL / TLS
  - Bitcoin
- Attacks on cryptography

Security \si-ˈkyůr-ə-tē\

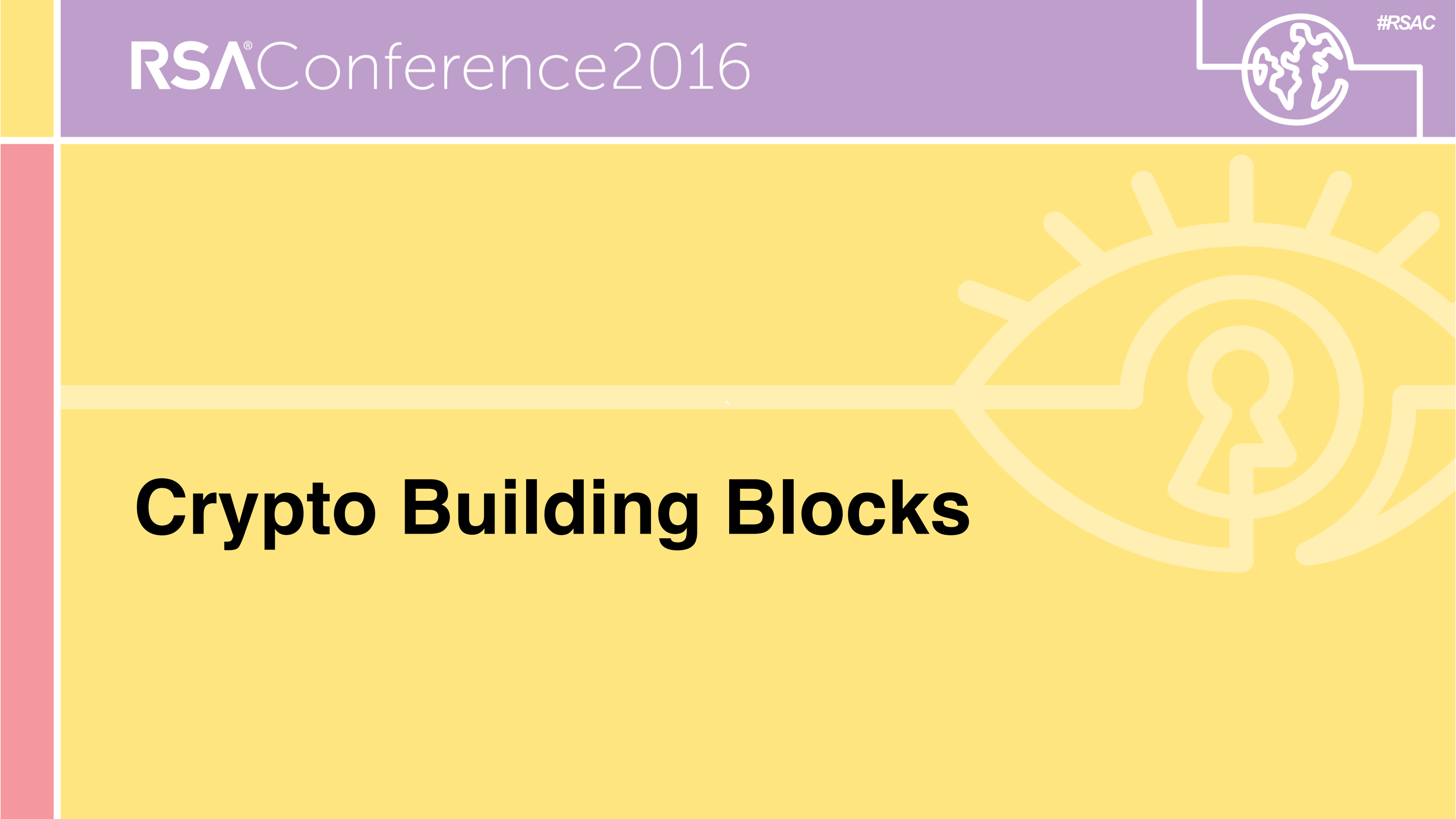
the state of being free from danger or threat

Cryptography terms

- Confidentiality
- Integrity
- Authentication
- Access control
- Non-repudiation

Other Criteria

- Interoperability
- Performance
- Usability

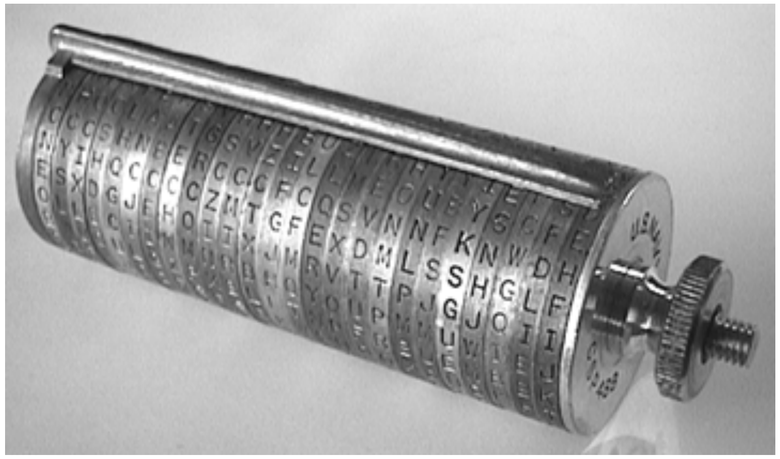


Crypto Building Blocks

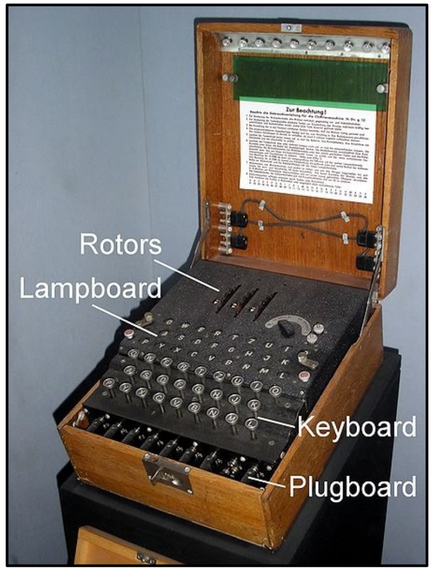
Encryption

Obfuscation that is fast when you know the secrets, but impossible or slow when you don't.

Scytale
300BC



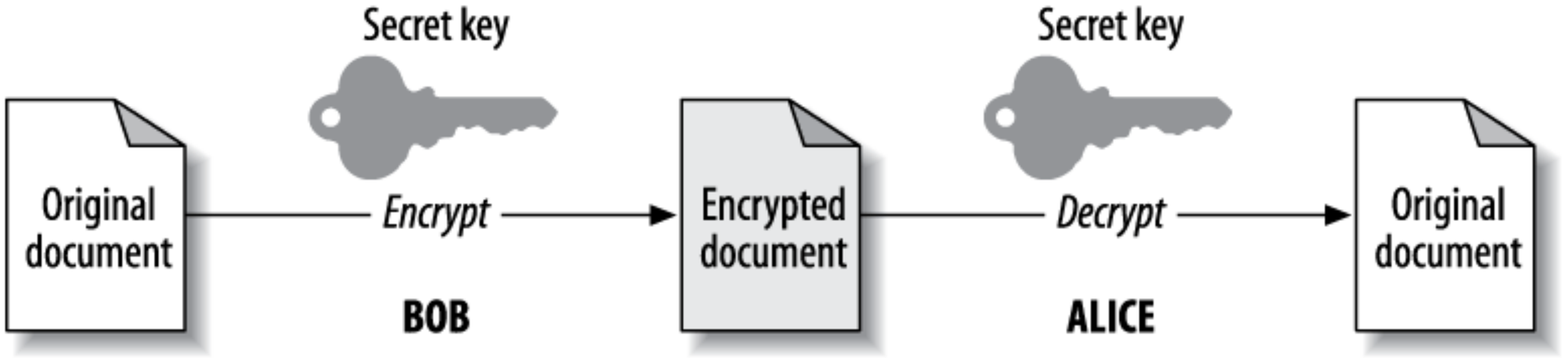
Jefferson Wheel (M94)
1900s



Enigma Machine
1920s

Image credit: Luringen, Sobebunny, R Bo

Symmetric encryption

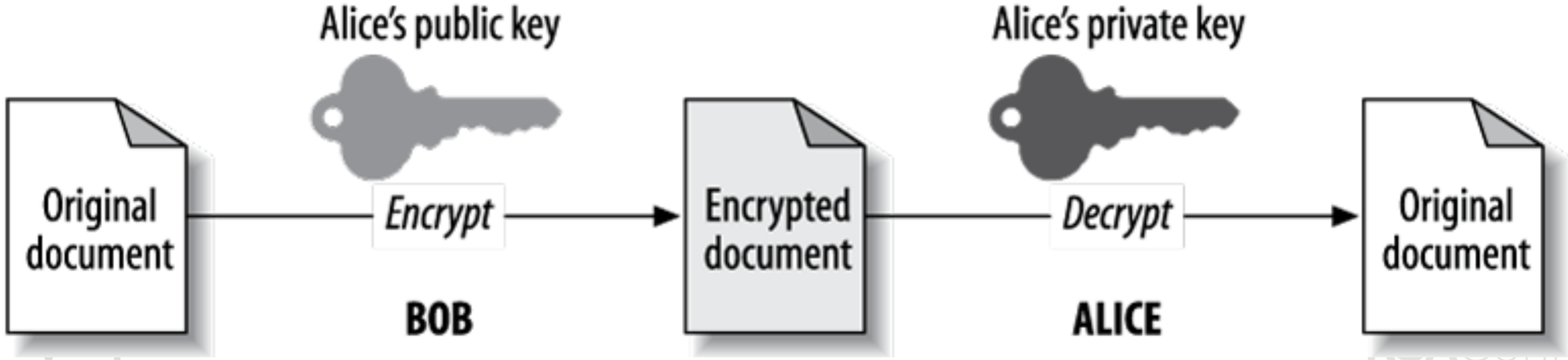


- Use shared key to encrypt/decrypt
  - Algorithm does not need to be secret
  - Key must be agreed and communicated in advance
- Convenient and fast
- Examples: RC4, 3DES, AES

Asymmetric encryption

Two related keys: one private, one public

- Anyone with the public key can encrypt the message
- Only the private key holder can decrypt message
- Enables encryption, key exchange, and authentication
  - Examples: RSA, Diffie-Hellman, ElGamal, DSA, Elliptic curve (ECDH / ECDSA)
  - Significantly slower than symmetric encryption



Authentication

Confirm data integrity and message origin

Egyptian signet ring
(500BC)

Mark of the Fisherman
(1200AD)

On death, Cardinal Camerlengo to destroy

US nuclear "football"
(present day)

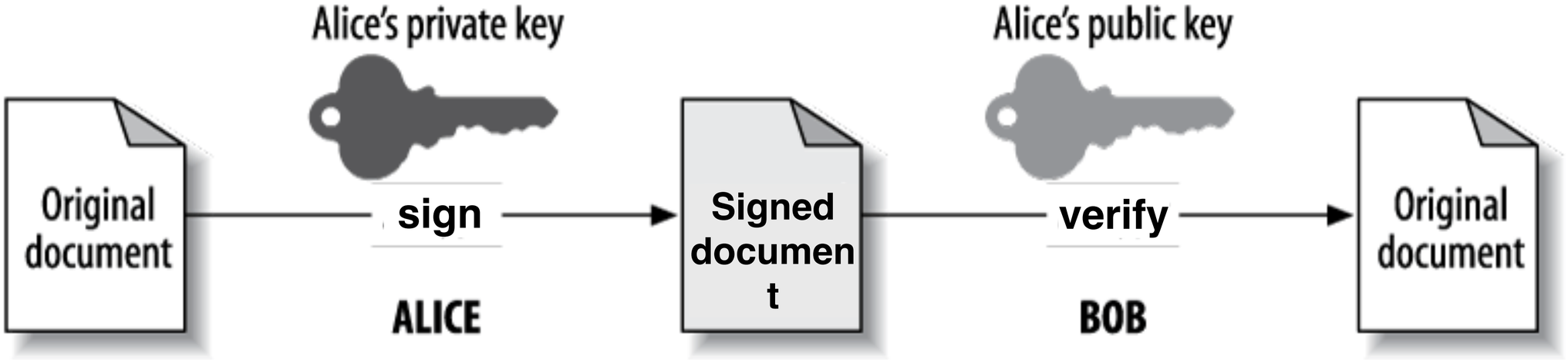
Keys roll at noon on inauguration day

British Museum, flikr:favoritethings

Digital signatures

Asymmetric cryptography can authenticate messages

- Only the private key holder can generate a signature
- Anyone with the public key can validate the signature
- Signatures protect **digital certificates** from modification or forgery



Digital certificates

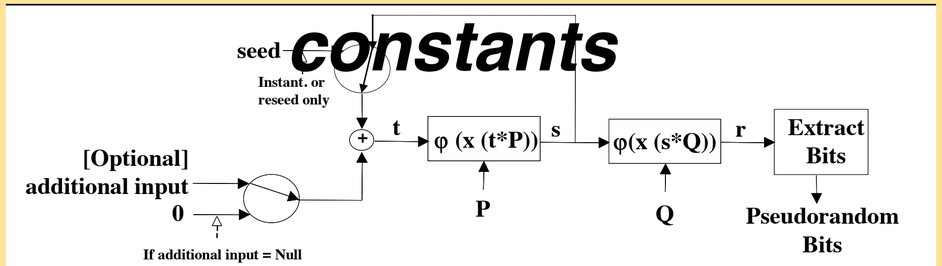
- Digital ID can include public/private keypair
- **Digital certificate** conveys identity
  - Credential holder info (name, address, etc.)
  - Identity's public key
  - Validity period
  - Digital signature of Certificate Authority (CA)
- Authentication has 3 steps
  - CA signature confirms data is authentic, vouched for
  - Do we approve of data in the certificate?
  - Identity keypair validated to confirm ID holder has the private key

Randomness matters

- Random numbers at heart of crypto
  - Used for key generation
  - Weak keys = weak encryption

- Random number generators
  - True random (TRNG) – *truly random*
  - Pseudorandom (PRNG) – *look random*
    - PRNGs fine <u>if properly seeded, properly designed</u>

*NIST SP800-90A: Dual EC DRBG with ~~NIST~~ NSA**



constants

A.1.1 Curve P-256

p = 115792089210356248762697446949407573530086143415290314195533631308867097853951

n = 115792089210356248762697446949407573529996955224135760342422259061068512044369

b = 5ac635d8 aa3a93e7 b3ebbd55 769886bc 651d06b0 cc53b0f6 3bce27d2604b

Px = 6b17d1f2 e12c4247 f8bce6e5 63a440f2 77037d81 2deb33a0 f4a13945 d898c296

Py = 4fe342e2 fe1a7f9b 8ee7eb4a 7c0f9e16 2bce3357 6b315ece cbb64068 37bf51f5

Qx = c97445f4 5cdef9f0 d3e05e1e 585fc297 235b82b5 be8ff3efca67c598 52018192

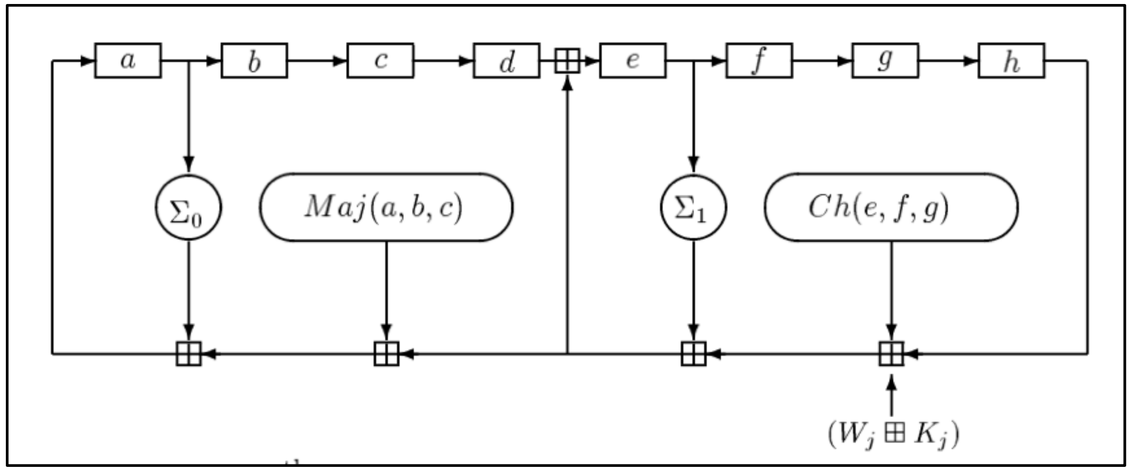
Qy = b28ef557 ba31dfcb dd21ac46 e2a91e3c 304f44cb 87058ada 2cb81515 1e610046

(don't use these)

* NYT Snowden memos, September 2013

Hash functions

- One-way transformation to generate *data fingerprints* for:
  - Digital signatures
  - Integrity validation
  - Tokenization (e.g., storing passwords)



SHA2 (SHA-256) compression function

- Examples
  - MD5 **considered broken**
  - SHA-1 (160) **some concerns**
  - SHA-2 (256) **ok**
  - Keccak and SHA-3

Desirable qualities

- Preimage resistance (one-wayness
- Collision resistance and birthday

Stay humble

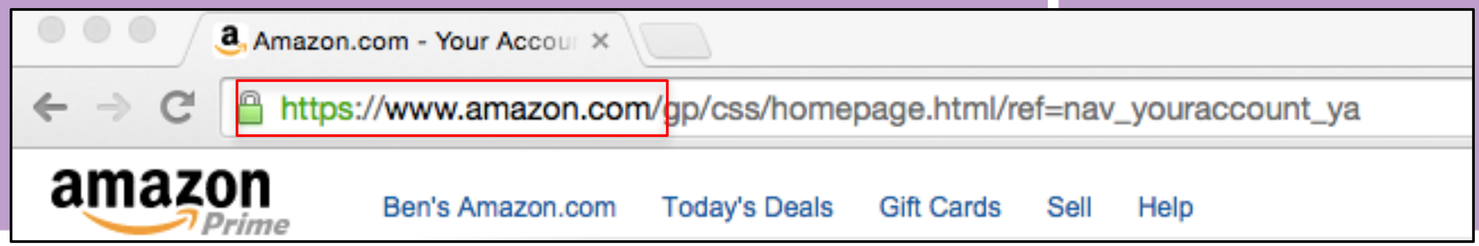
- Don’t roll your own crypto
  - Failure modes subtle, catastrophic
  - Standard crypto has been strongly vetted
- Avoid unnecessary complexity
  - System only as strong as its weakest link
  - Complexity = more stuff to go wrong
- Never rely on obscurity
  - “If I can barely understand it, then it must be strong!”
  - Kerckhoffs's principle: only the key should be secure

Auguste Kerckhoffs (1835-1903)

Putting It All Together

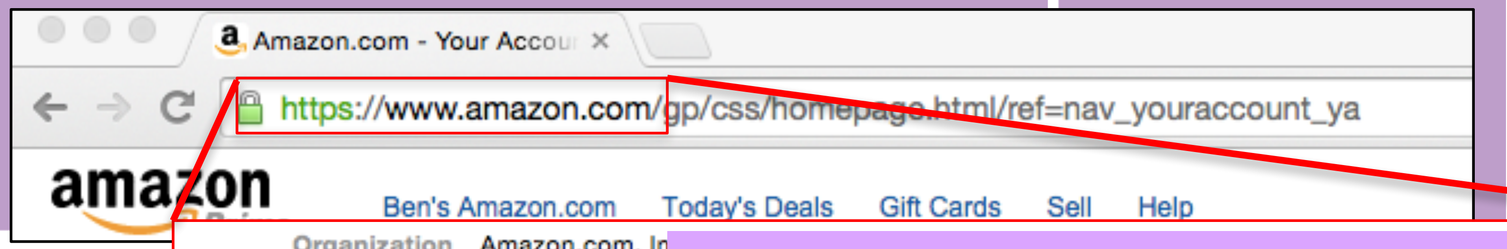
- SSL / TLS
- Bitcoin

TLS

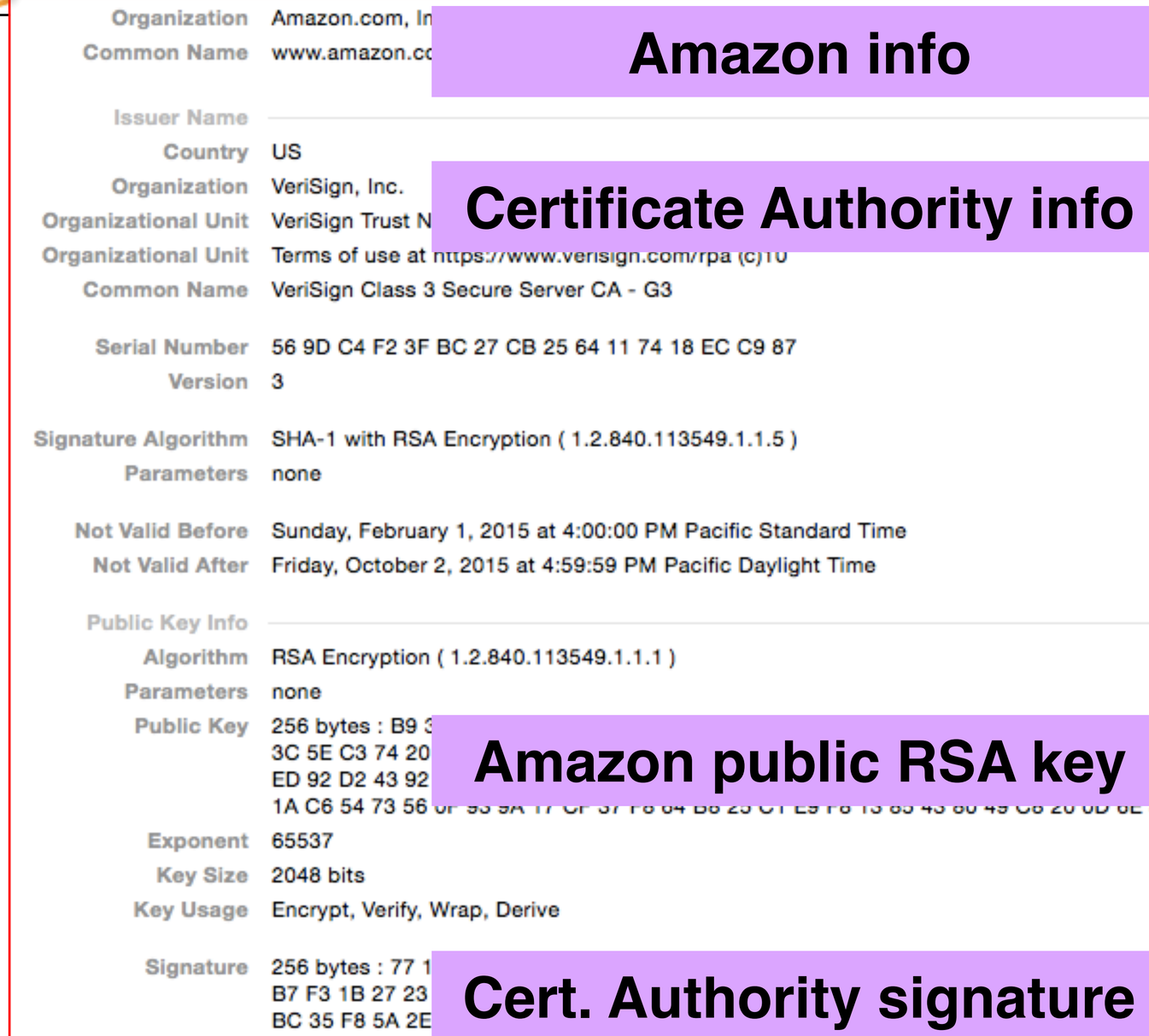


- Transport Layer Security
  - World's most widely used cryptographic protocol
  - From Netscape SSL3 (Kocher, 1995)
- Security requirements
  - Securely connect with someone you have never met
  - Data privacy, data integrity, no site impersonation, no man-in-middle

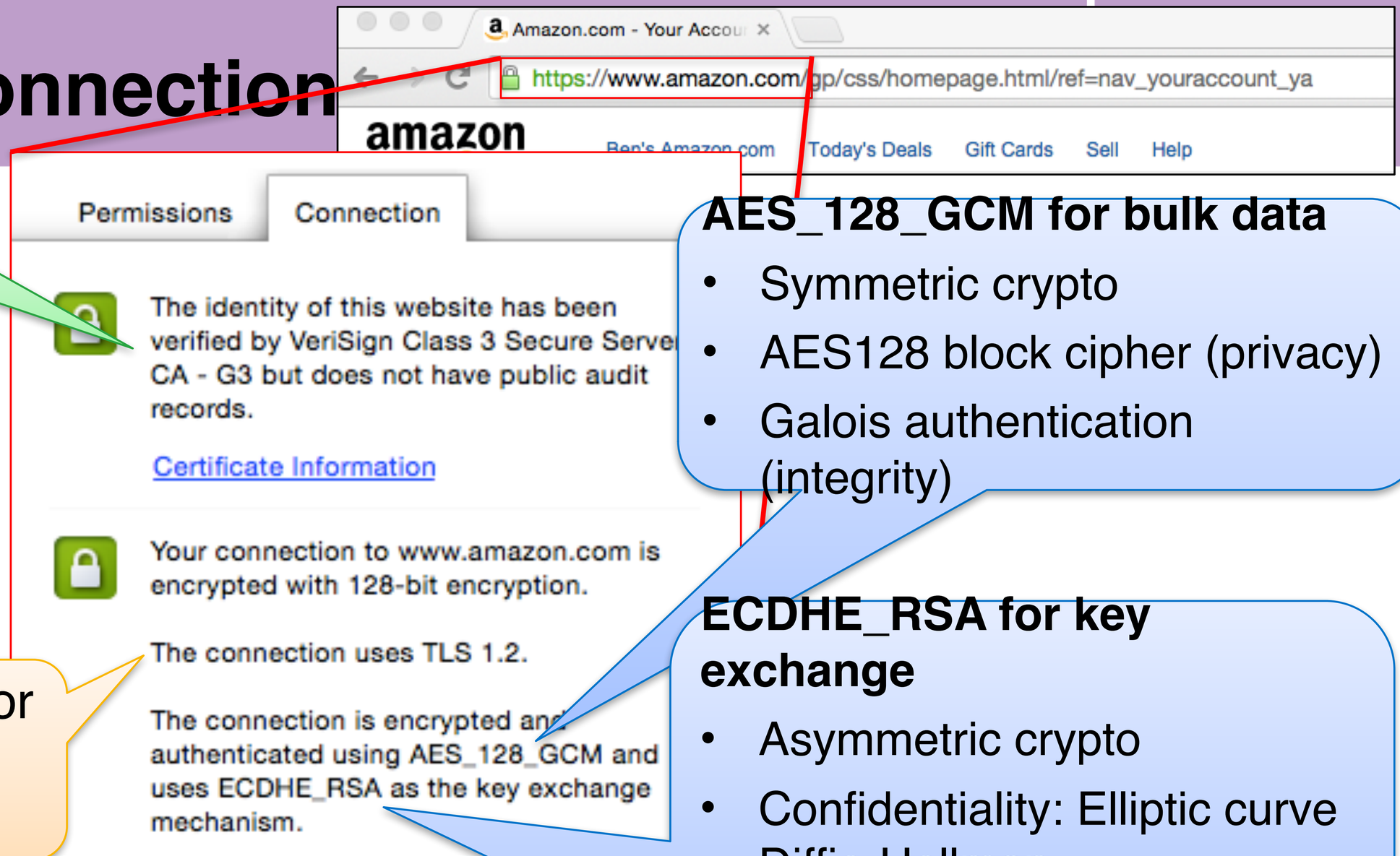
Getting to https



1. Webserver provides digital certificate to browser
   - "Amazon.com's passport"
2. TLS layer + browser "authenticates passport"
   - Confirms data fields in cert
   - Confirms digital signature
3. TLS layer confirms that webserver holds private key
   - Sends encrypted data that can only be decrypted w/private key



TLS: Connection



Certificate check passed!

TLS 1.2 protocol for secure socket & session mgmt

AES_128_GCM for bulk data

- Symmetric crypto
- AES128 block cipher (privacy)
- Galois authentication (integrity)

ECDHE_RSA for key exchange

- Asymmetric crypto
- Confidentiality: Elliptic curve Diffie-Hellman
- Authentication: RSA2048
- “Perfect forward secrecy”

Bitcoin (1/2)

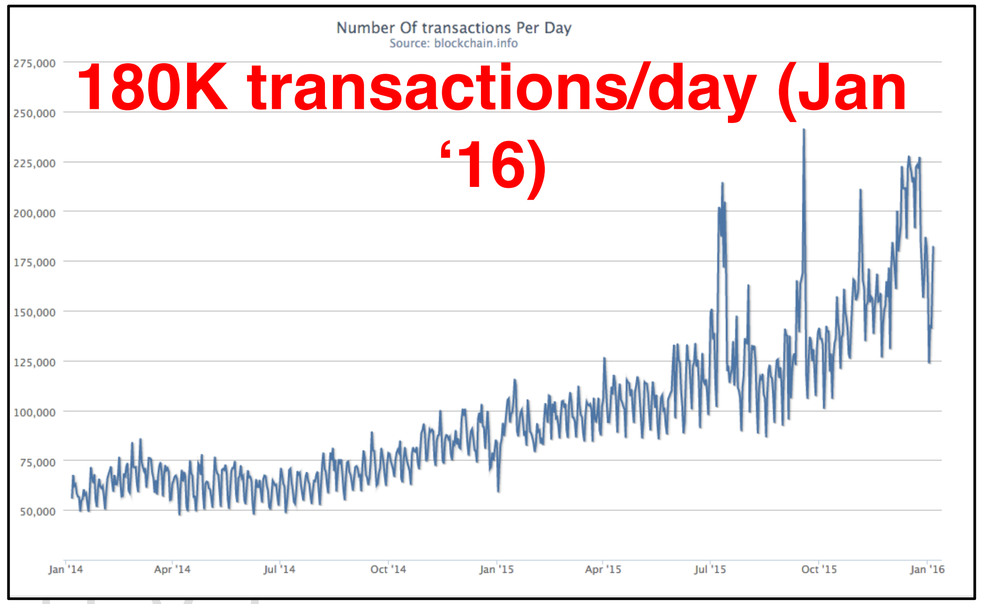
Peer-to-peer, decentralized currency

- Not underwritten by any entity
- “Satoshi Nakamoto” paper (2008)

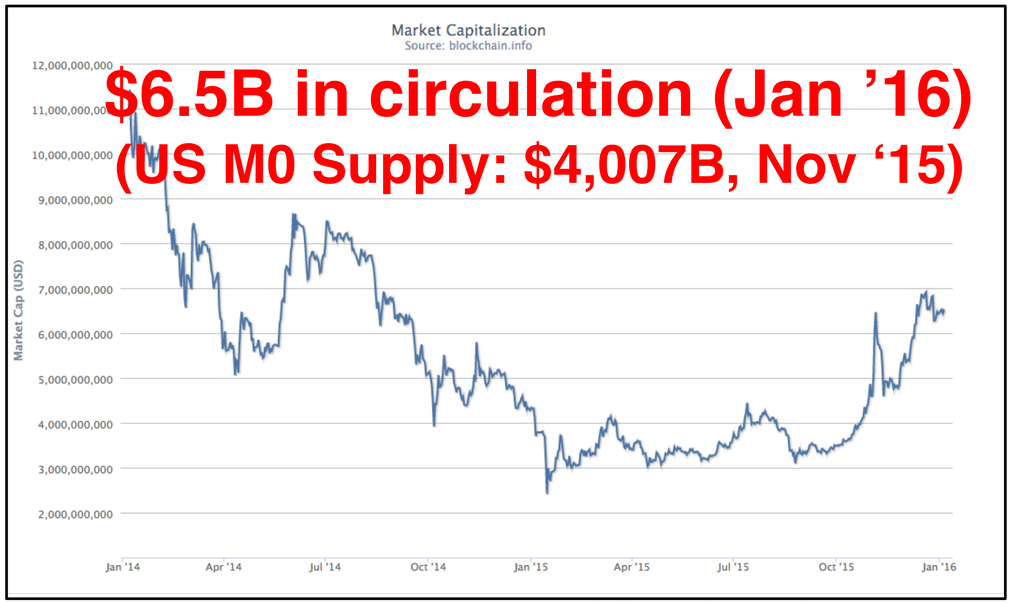
Bitcoin: A Peer-to-Peer Electronic Cash System

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



180K transactions/day (Jan ‘16)



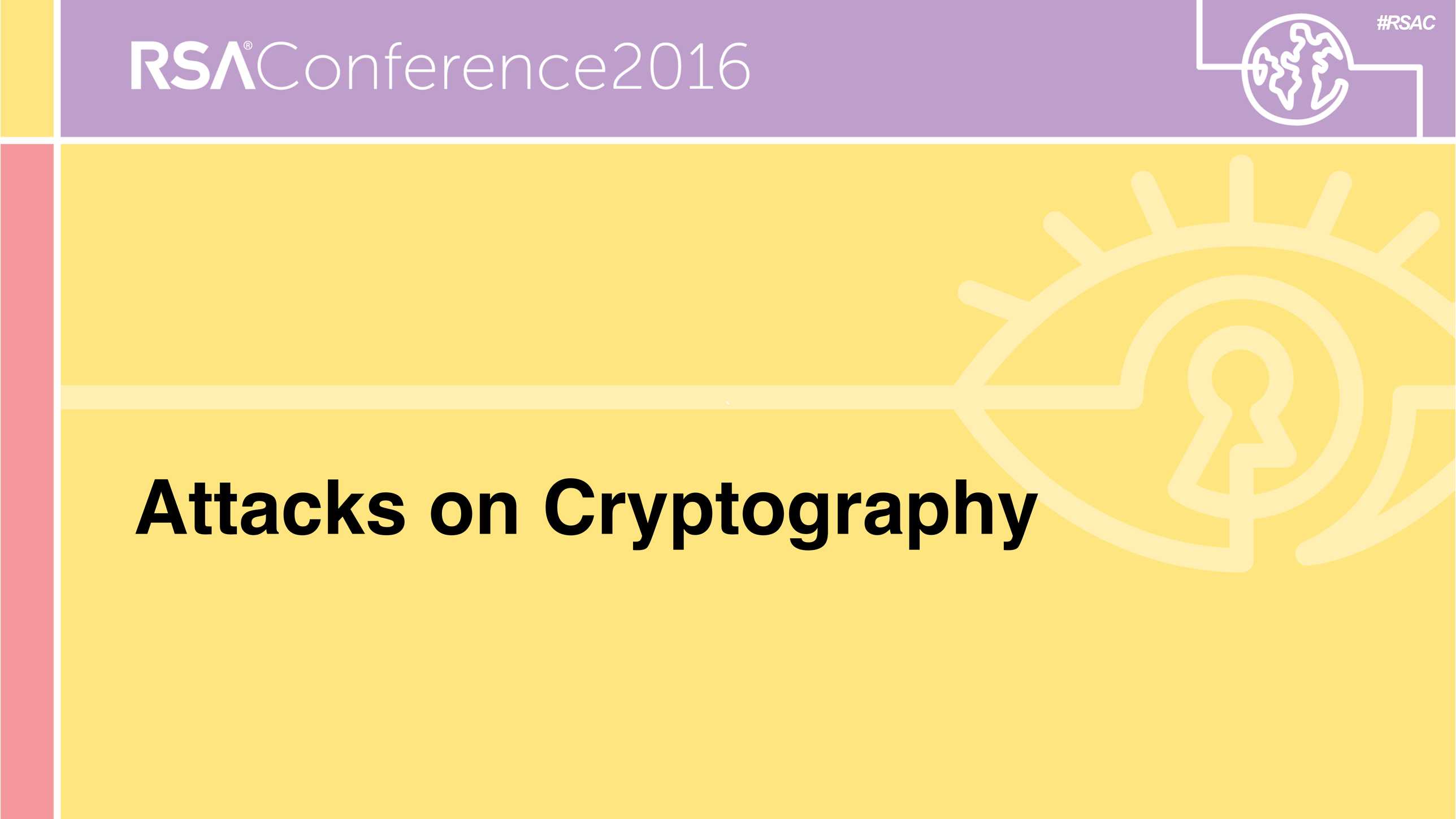
$6.5B in circulation (Jan ’16)
(US M0 Supply: $4,007B, Nov ‘15)

Diagrams from blockchain.info

Bitcoin (2/2)

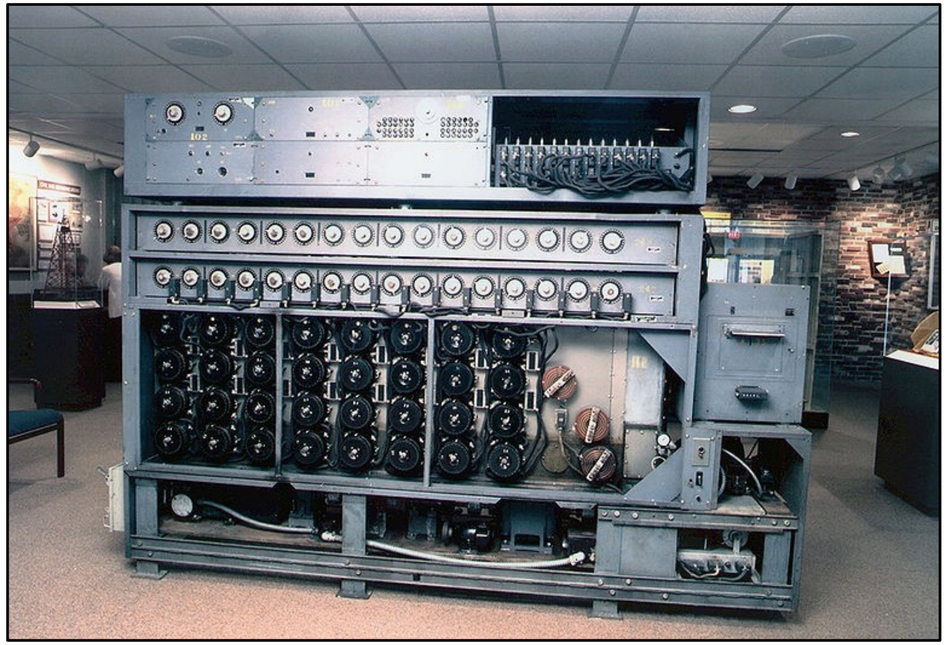
Characteristic	What happens	Cryptography
Value creation	Mined by searching for magic values ***KWh —> BTC!***	**Proof-of-work** method uses **SHA-256 hash function**
Coin transfers	Digital signatures	**ECDSA digital signature**
Recordkeeping (no double-spending)	Distributed ledger with financial incentive for a “single view”	**Block chain** uses **SHA-256 hash function**
Backing entity	**NONE!**	*Everything regulated by **market forces** + **math**!*

Great technical resource: Bitcoin Developer Reference by Krzysztof Okupski



Attacks on Cryptography

Brute force



US Navy Bombe, 1943

Contains 16 four-rotor Enigma equivalents to perform exhaustive key search.

DES Keysearch Machine, 1998

Tests 90 billion keys/sec, average time to crack 56-bit DES: **5 days**

(Cryptography Research, AWT, EFF)

Cryptanalysis

- HDCP = “High bandwidth Digital Copy Protection”
- Protects digital content, interoperability
  - Fast, offline, any-to-any negotiation
  - Encryption and authentication
- “Clever” key management
  - No one device contains global secret
  - HDCP master key published (2010)
  - **Unlicensed implementations cannot be revoked**

Number of KSVs	40	42	44	46	48	50
Prob. of Spanning M	.295	.773	.940	.982	.997	.999

But keys from ~40 devices can reveal the master key

A Cryptanalysis of the High-bandwidth Digital Content Protection System
(Crosby, Goldberg, Johnson, Song, Wagner)

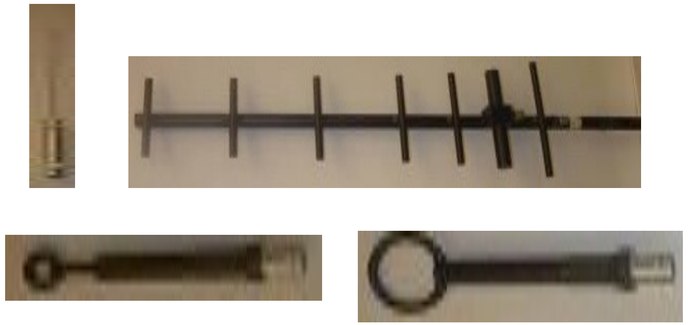
image from www.hdmi.org

Implementation: Side Channel (1/2)

Simple EM attack with radio at distance of 10 feet

Devices

Antennas



Digitizer,
GNU Radio peripheral
($1000)

Receiver ($350)

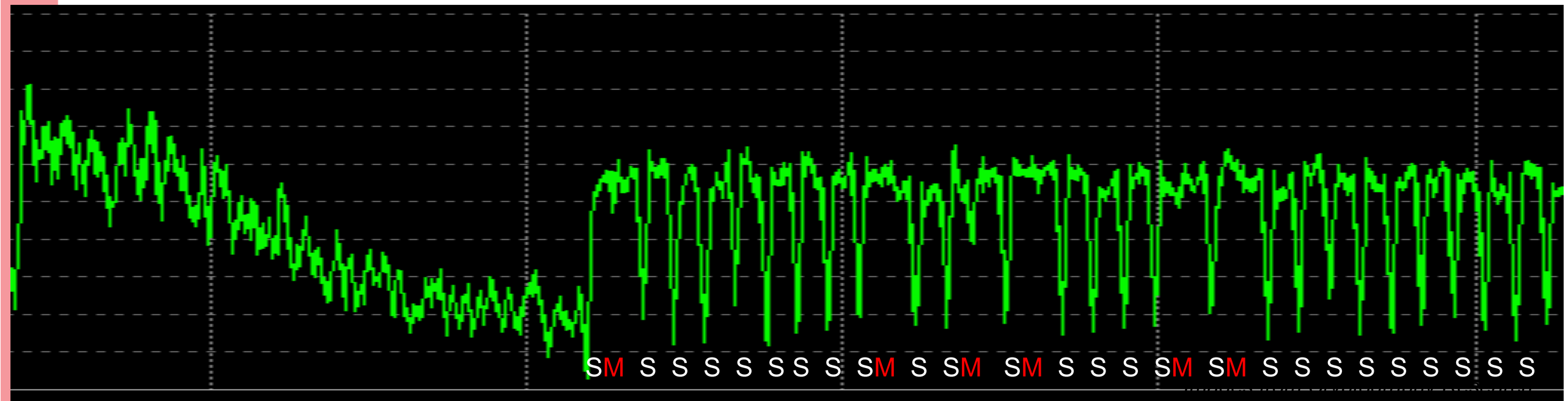
Signal Processing
(demodulation, filtering)

Images from Cryptography Research

Implementation: Side Channel (2/2)

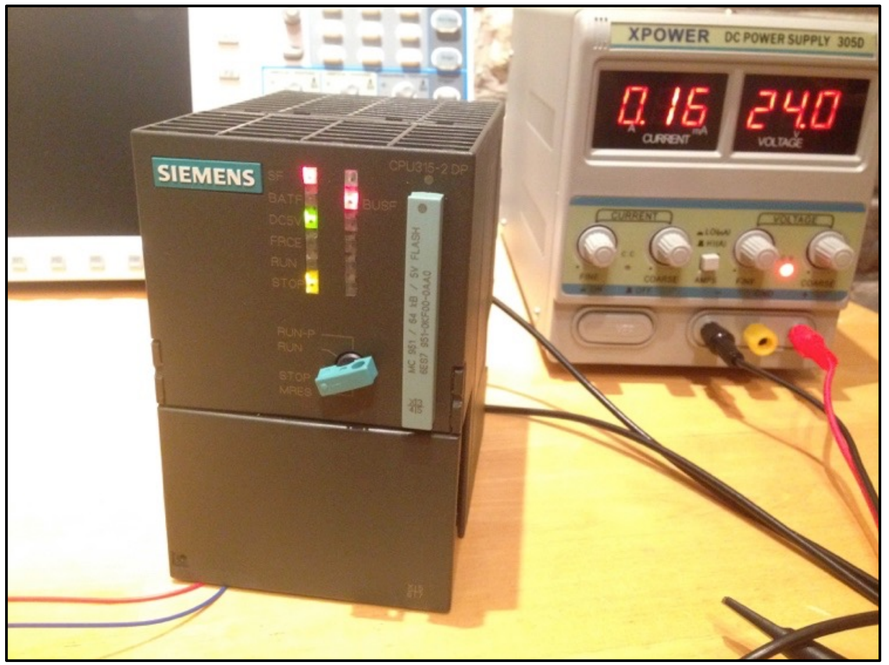
Focus on Mp^{dp} mod p calculation (Mq^{dq} mod q similar)

```
For each bit i of secret dp
   perform "Square"
   if (bit i == 1)
     perform "Multiply"
   endif
endfor
```



Crypto necessary, but not sufficient

Game King poker (2014)
Bug allows user to adjust bet
after hand played

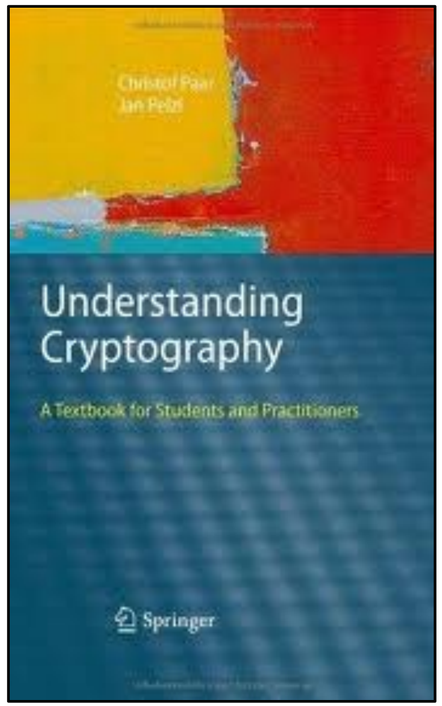


Siemens Simatic S7-315
Target of ~~Stuxnet~~
Operation Olympic Games

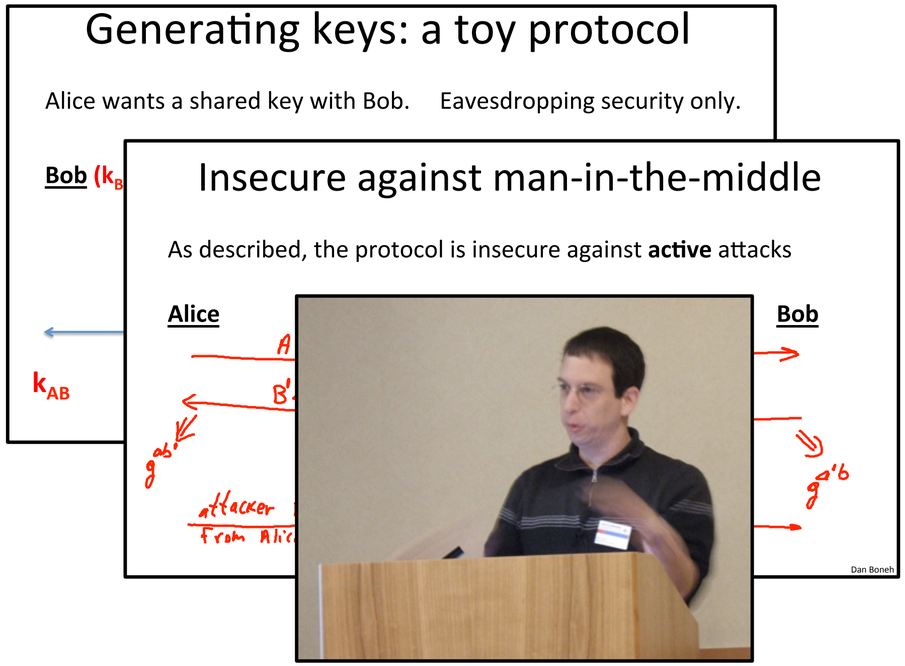
http://www.wired.com/2014/10/cheating-video-poker/

Learn More!

Resources



Understanding Cryptography
Christof Paar and Jan Pelzl
(Springer, 2009)



Cryptography online course
Dan Boneh, Stanford University

How to apply what you have learned

- In the first three months:
  - Identify where cryptography is used in your organization
  - Identify infrastructure required (key management, certificates)

- Within six months:
  - Know what crypto **can** do. Explain the different security properties.
  - Know what crypto **can't** do. Understand basic implementation security issues.

Questions?

HVF

@ Benjamin Jun

Friday March 4, 10:10am

Our Road Ahead: Today's Tech Developments, Tomorrow's Security Challenges

Fireside chat with Benjamin Jun and Hugh Thompson
Industry Experts EXP-F02