An Invitation to Cryptography

CMSC 23200/33250, Autumn 2018, Lecture 2

David Cash

University of Chicago


6V
断
45V

nothing

Today 11:11

Can you please come over asap to help me move the couch?

I need to be out of here by 3pm

I guess you forgot your phone at home or something

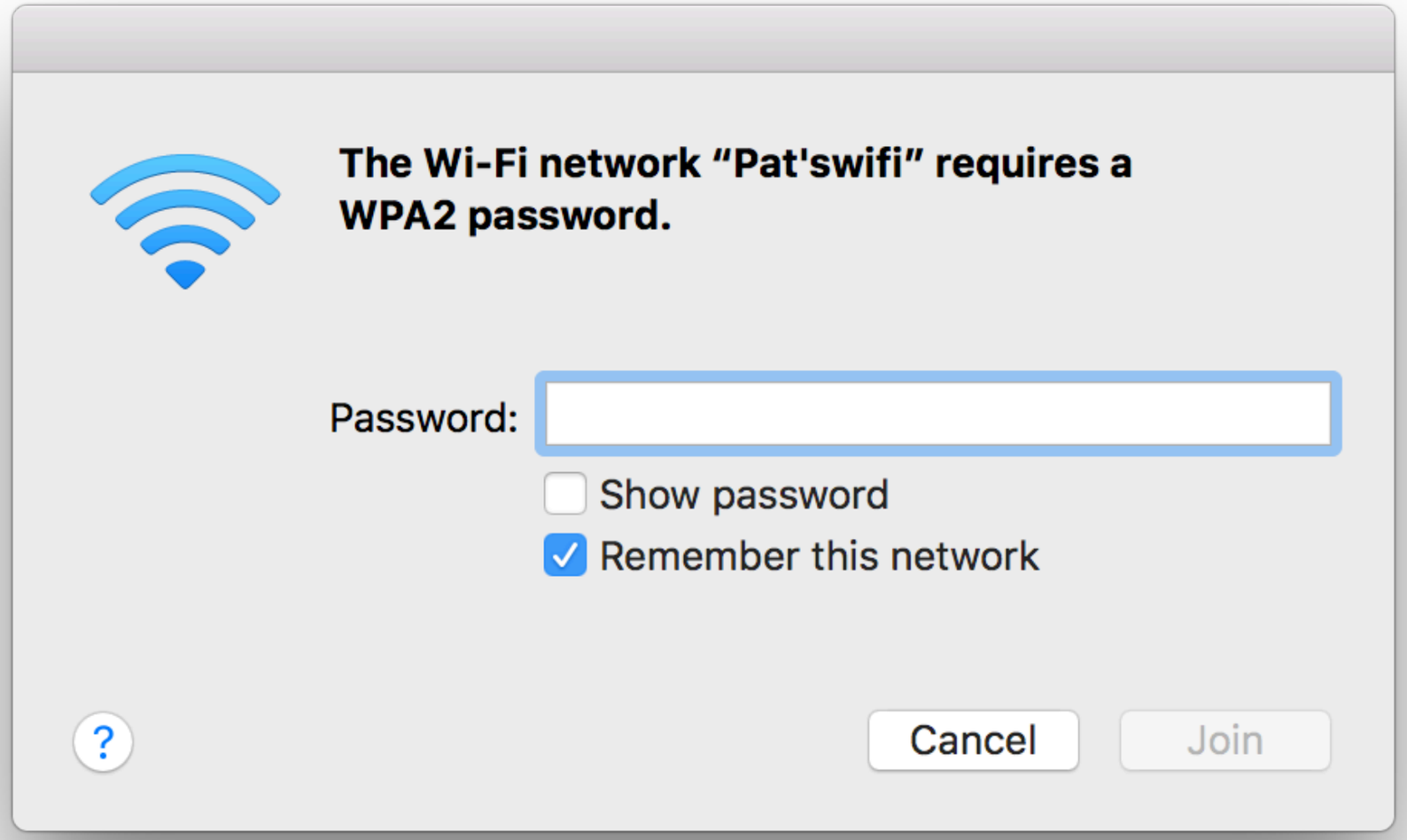
Delivered

Send

iMessage

5100 21

5100


The Wi-Fi network “Pat'swifi” requires a WPA2 password.
Password:
Show password
Remember this network
?
Cancel
Join

Amazon.com: Online Shopp

https://www.amazon.com

www.amazon.com

Your connection to this site is private.

Details

Permissions | Connection

Chrome verified that Symantec Class 3 Secure Server CA - G4 issued this website's certificate. The server did not supply any Certificate Transparency information.

Certificate Information

Your connection to www.amazon.com is encrypted using a modern cipher suite.

The connection uses TLS 1.2.

The connection is encrypted and authenticated using AES_128_GCM and uses ECDHE_RSA as the key exchange mechanism.

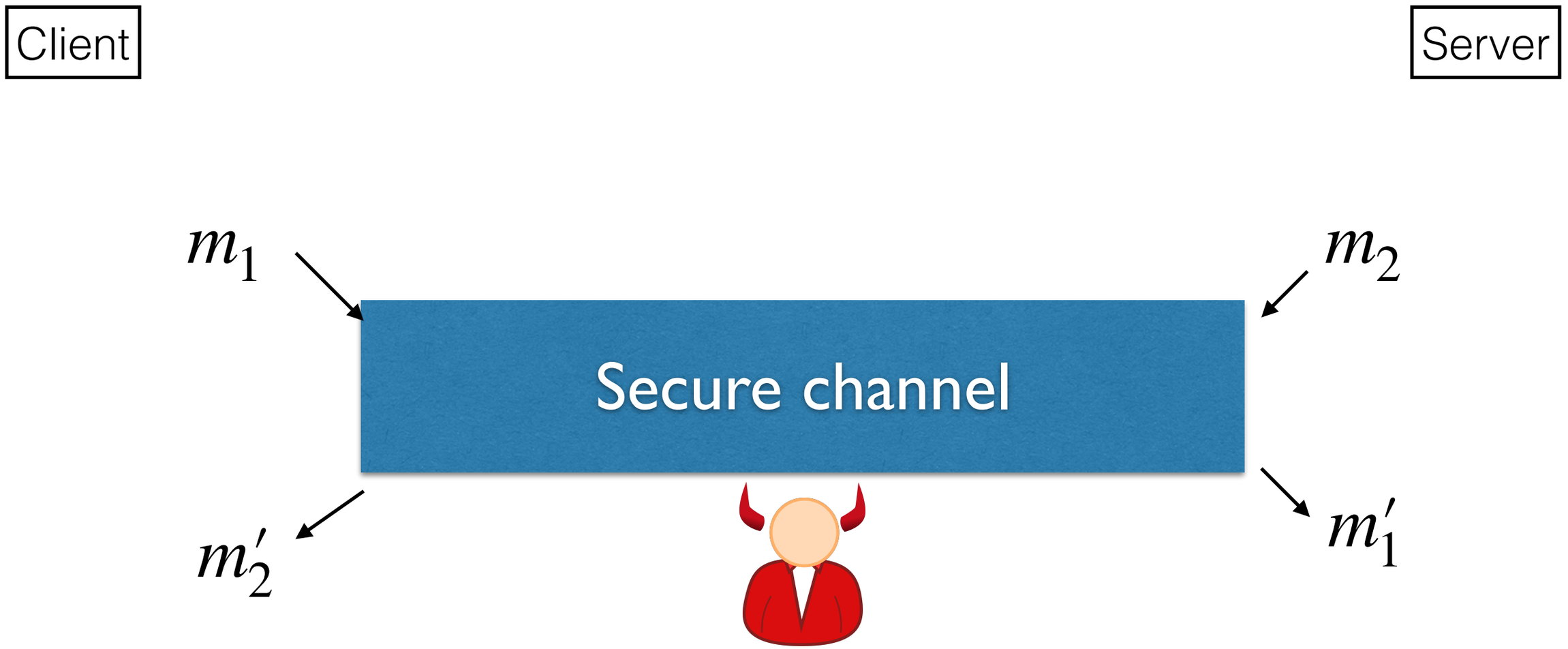
What do these mean?

What is Cryptography?

Cryptography involves algorithms with security goals.

Cryptography involves using math to stop adversaries.

Common Security Goal: Secure Channel



Confidentiality: Adversary does not learn anything about messages m_1, m_2

Authenticity: $m_1' = m_1$ and $m_2' = m_2$


Warning: subtitles abound


WEP/WPA1,2: Secure WiFi

pw=“fourwordsuppercase”

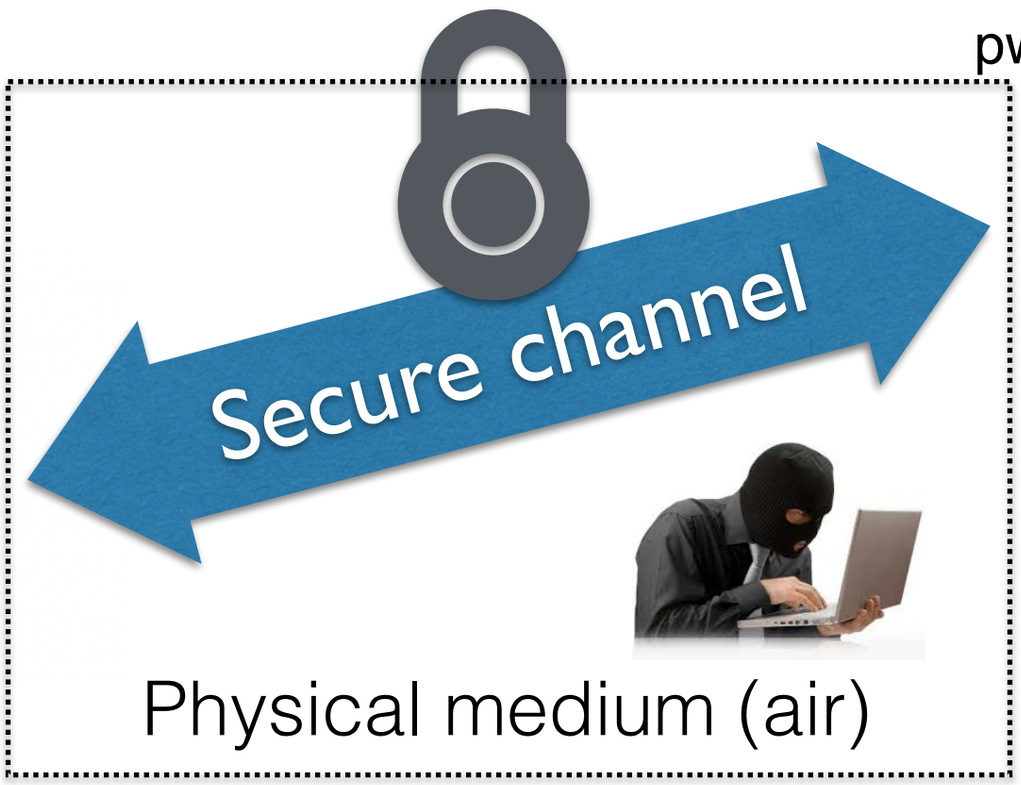
Yo, w

… nevermind

It’s four words uppercase,
one word, lowercase.

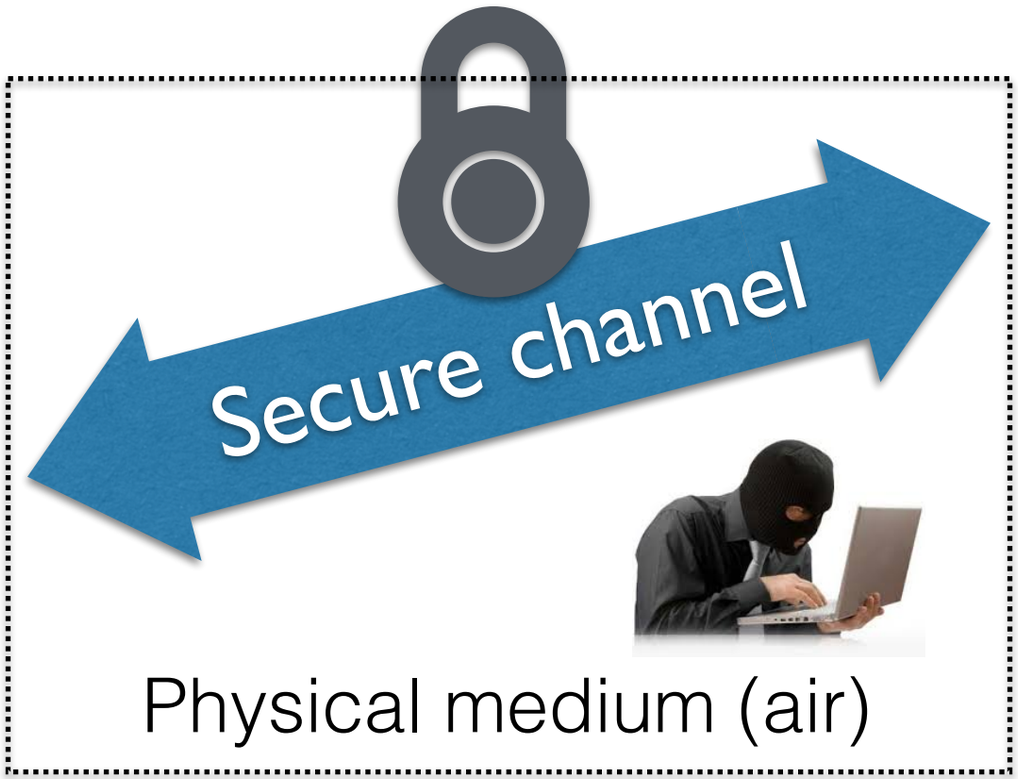
WPA2 (Wi-Fi Protected Access 2): Secure WiFi

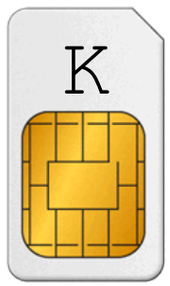
pw="fourwordsuppercase"



pw="fourwordsuppercase"

GSM Cell Phone Encryption (A5/1, A5/3)





K = b9842544

User	Key
Alice Doe	340934c3
Betty Lee	b9842544
Cheryl Zang	93d94520
Pat Dobbs	2ea0f48d
…	…

Crypto in your browser: TLS (Transport Layer Security)

TLS MAGIC

Secure channel

Internet

amazon

Time to pull the trigger and
buy that Boyfriend Pillow
I've had my eye on…

Crypto in your browser: TLS (Transport Layer Security)

TLS MAGIC

Secure channel

Internet

amazon

Broken by:

Actually TLS seems to work most of the time.

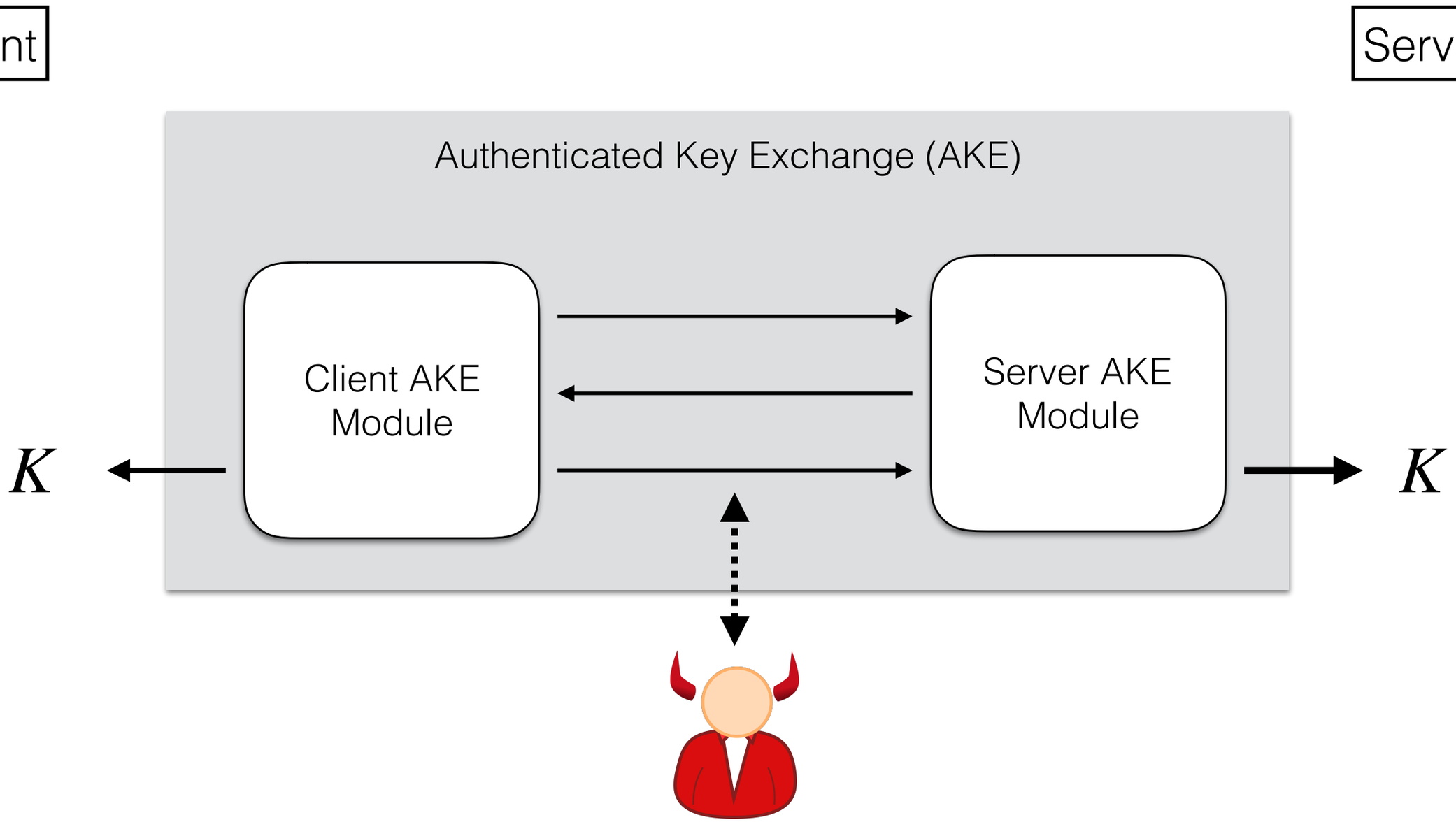
Used billions of times a day, supporting Internet and web.

Four settings for cryptography

Pre-shared key? \ Security Goal	Confidentiality	Authenticity
Symmetric	Symmetric Encryption (aka Secret-key Encryption)	Message Authentication Code (MAC)
Asymmetric	Asymmetric Encryption (aka Public-key Encryption)	Digital Signatures

Now: A tour of TLS, which uses all 4.

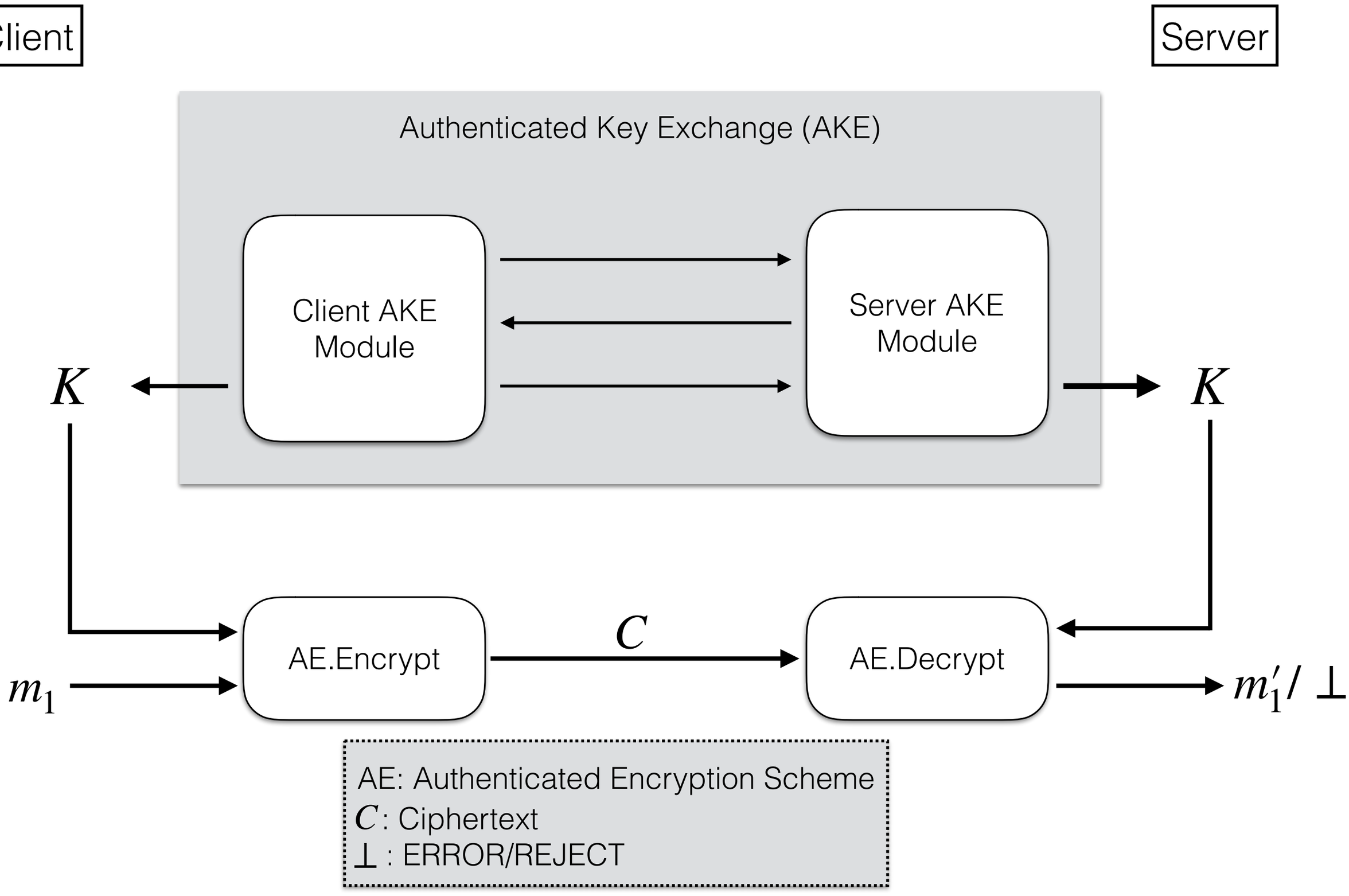
TLS Cryptographic Core



K should be a fresh random and authentic session key

Adversary should not be able to influence or know K

TLS Cryptographic Core

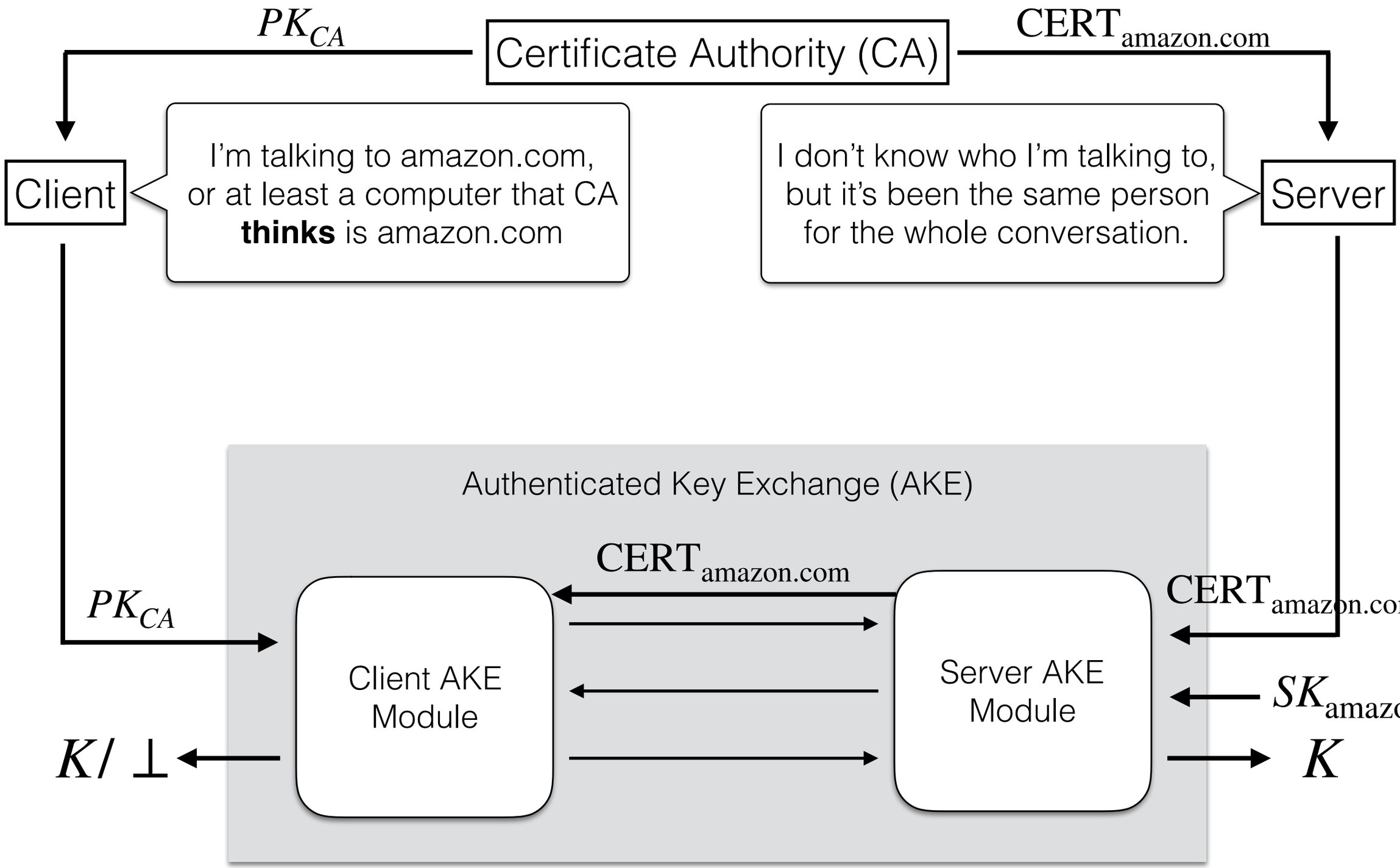


What does it mean to **really** talk to amazon.com?

Messages were emitted by machine owned by Amazon.com Inc.

Messages were emitted by machine with IP address associated to amazon.com by DNS.

I'm getting my boyfriend pillow *like now.*



$\text{CERT}_{\text{amazon.com}}$: amazon.com certificate issued by CA

PK_{CA} : CA's public key

$SK_{\text{amazon.com}}$: amazon.com's secret key tied to $\text{CERT}_{\text{amazon.com}}$

Certificate Authorities

IdenTrust™ IDENTITY ASSURED

COMODO

Let's Encrypt

digicert®

Hundreds more, some with dubious security practices.

8/30/2011
12:40 PM

Kelly Jackson Higgins

Digital Certificate Authority Hacked, Dozens Of Phony Digital Certificates Issued

DigiNotar confirms it was breached and Google.com just one of 'several dozens' of fraudulently issued digital certificates obtained by hackers and now revoked

amazon.com

ionic-vpn gm gcal reader gdocs sheets gdrive tw NYT SCN'16 PC TCC'16b PC CCS'16 PC weather RU banks xword Encrypted st...ge companies

Safari is using an encrypted connection to www.amazon.com.

Encryption with a digital certificate keeps information private as it's sent to or from the https website www.amazon.com.

- DigiCert Global Root G2
  - DigiCert Global CA G2
    - www.amazon.com

www.amazon.com
Issued by: DigiCert Global CA G2
Expires: Friday, March 29, 2019 at 7:00:00 AM Central Daylight Time
This certificate is valid

▶ **Trust**

▼ **Details**

Subject Name	
Country	US
State/Province	Washington
Locality	Seattle
Organization	Amazon.com, Inc.
Common Name	www.amazon.com
Issuer Name	
Country	US
Organization	DigiCert Inc
Common Name	DigiCert Global CA G2
Serial Number	07 DC 7D 69 44 60 E6 47 B7 6C 6E 78 E8 59 62 00
Version	3
Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters	None
Not Valid Before	Tuesday, March 27, 2018 at 7:00:00 PM Central Daylight Time
Not Valid After	Friday, March 29, 2019 at 7:00:00 AM Central Daylight Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	None
Public Key	256 bytes : E7 93 5A 5E F0 25 E1 7E 06 DB 88 1D 23 85 8C D0 25 5B 8B F5 51 72 F8 88 79 F5 47 23 F1 7C 2B 03 4D D4 05 42 46 47 A2 6B CC 2F 9E 55 D2 0B 07 C5 D2 84 24 FA 5F A0 AD E3 F0 2F C7 68 1F 93 14 88 A9 06 64 F1 82 05 42 0E 90 D5 D4 6C 52 E4 D6 60 D9 4D 33 19 F2 13 82 9E 1D 13 F0 E2 43 01 DD 42 51 59 83 E9 74 1D 2E 69 A9 41 FC 8B 56 C7 01 AB 1A DE 9D 4C 13 63 65 92 37

? Hide Certificate OK

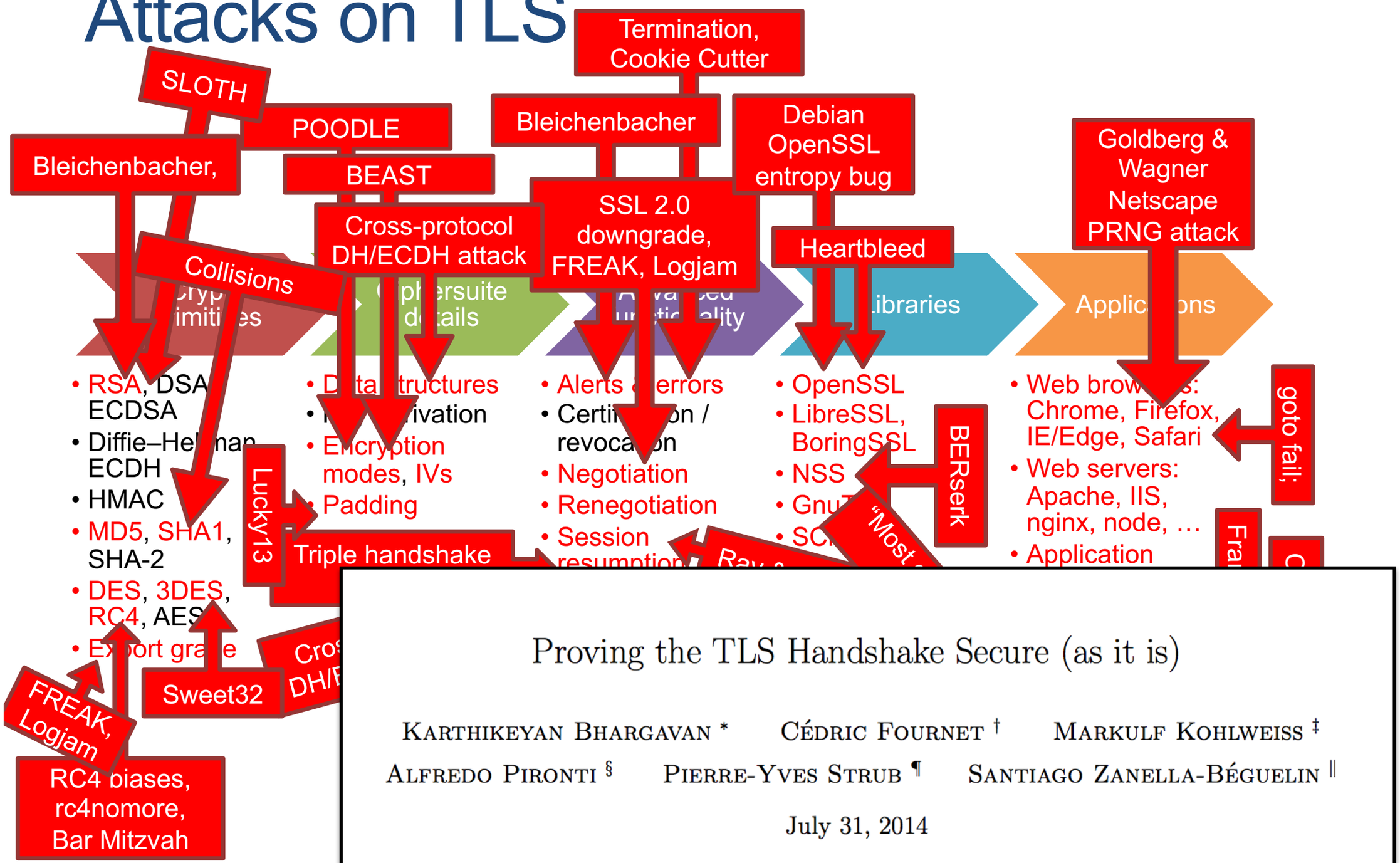
Deliver to Chicago

Cart

Back t

Shop all

Attacks on TLS

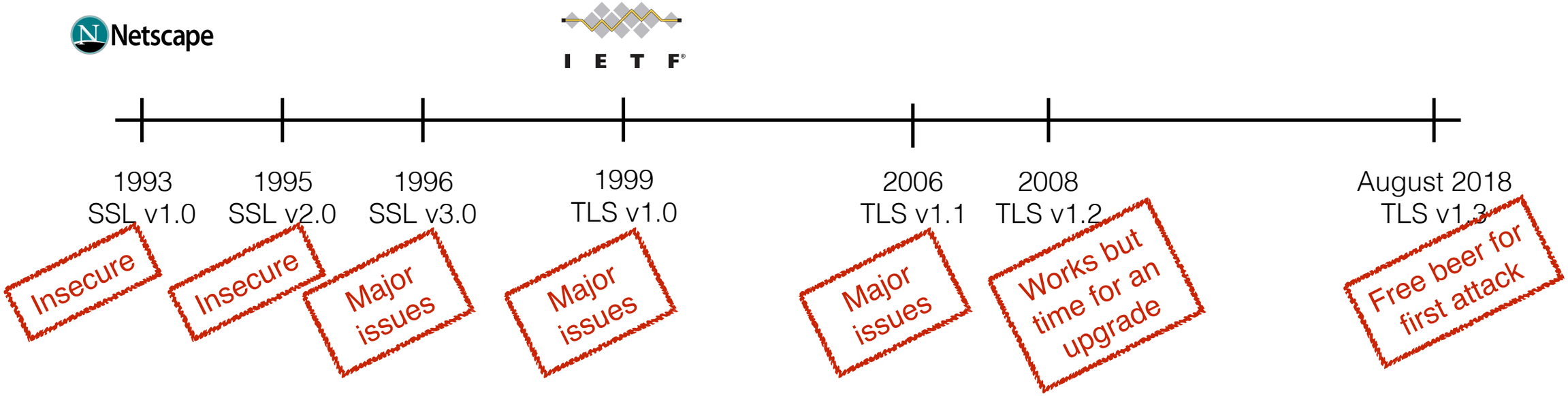


Proving the TLS Handshake Secure (as it is)

KARTHIKEYAN BHARGAVAN * CÉDRIC FOURNET † MARKULF KOHLWEISS ‡
ALFREDO PIRONTI § PIERRE-YVES STRUB ¶ SANTIAGO ZANELLA-BÉGUELIN ‖

July 31, 2014

TLS History



Grandma, TLS 1.3 zero round-trip time session resumption with perfect forward secrecy is soooo dated.

Back in my day we did four-way handshakes… both ways, in the snow! With subgroups of prime fields!

First deployments happening now!

Security

It's official: TLS 1.3 approved as standard while spies weep

Now all you lot have to actually implement it

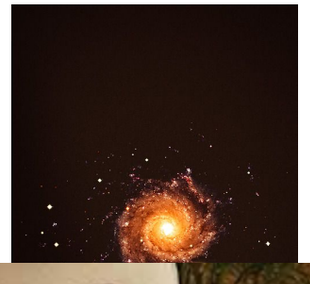
By Kieren McCarthy in San Francisco 13 Aug 2018 at 22:19 26 SHARE ▼

overhaul of a critical internet security protocol has been completed,
S 1.3 becoming an official standard late last week.

Crypto tools in TLS

Key Exchange
Public-Key Encryption
Trapdoor Function
Authenticated Encryption
Blockcipher
Stream cipher
Message Authentication Code
Digital Signature
Collision-Resistant Hash Function
…

Every interaction between pieces is an opportunity for an attacker.



Each has unique and subtle security properties

… all so we can buy boyfriend pillows securely

Crypto in CSMC 23200

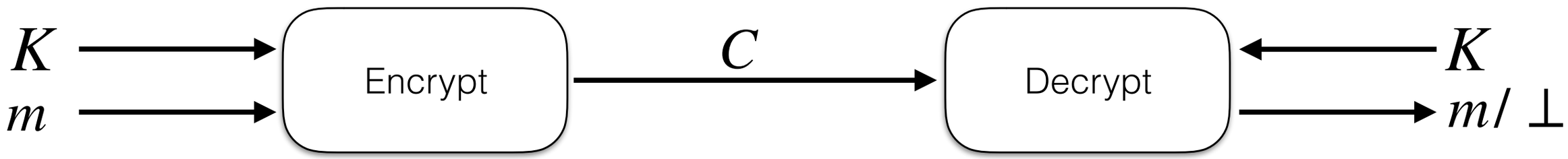
Symmetric Encryption (Lectures 2 & 3)
Symmetric Authentication and Hashing (Lecture 4 and 5)
Asymmetric Encryption (Lecture 6)
Digital Signatures (Lecture 7)
Putting it together: TLS (Lectures 8 & 9)

Rest of this lecture

- Syntax of a cipher
- Some historical ciphers and how they were broken
- The One-Time Pad cipher and its security/insecurity
- Towards practice: Begin stream ciphers and blockciphers

Cipher Syntax

A cipher is a pair of algorithms Encrypt, Decrypt:



Require that decryption recovers the same message.

Historical Cipher: ROT13 (“Caesar cipher”)

Encrypt(K,m): shift each letter of plaintext forward by K positions in alphabet (wrap from Z to A).

Plaintext: `DEFGH`
Key (shift): `3`
Ciphertext: `FGHKL`

Plaintext: `ATTACKATDAWN`
Key (shift): `13`
Ciphertext: `NGGNPXNGQNJA`

Historical Cipher: Substitution Cipher

Encrypt(K,m): Parse key K as a permutation π on {A,… Z}.
Apply π to each character of m.

P: `ATTACKATDAWN`

K: π →

C: `ZKKZAMZKYZGT`

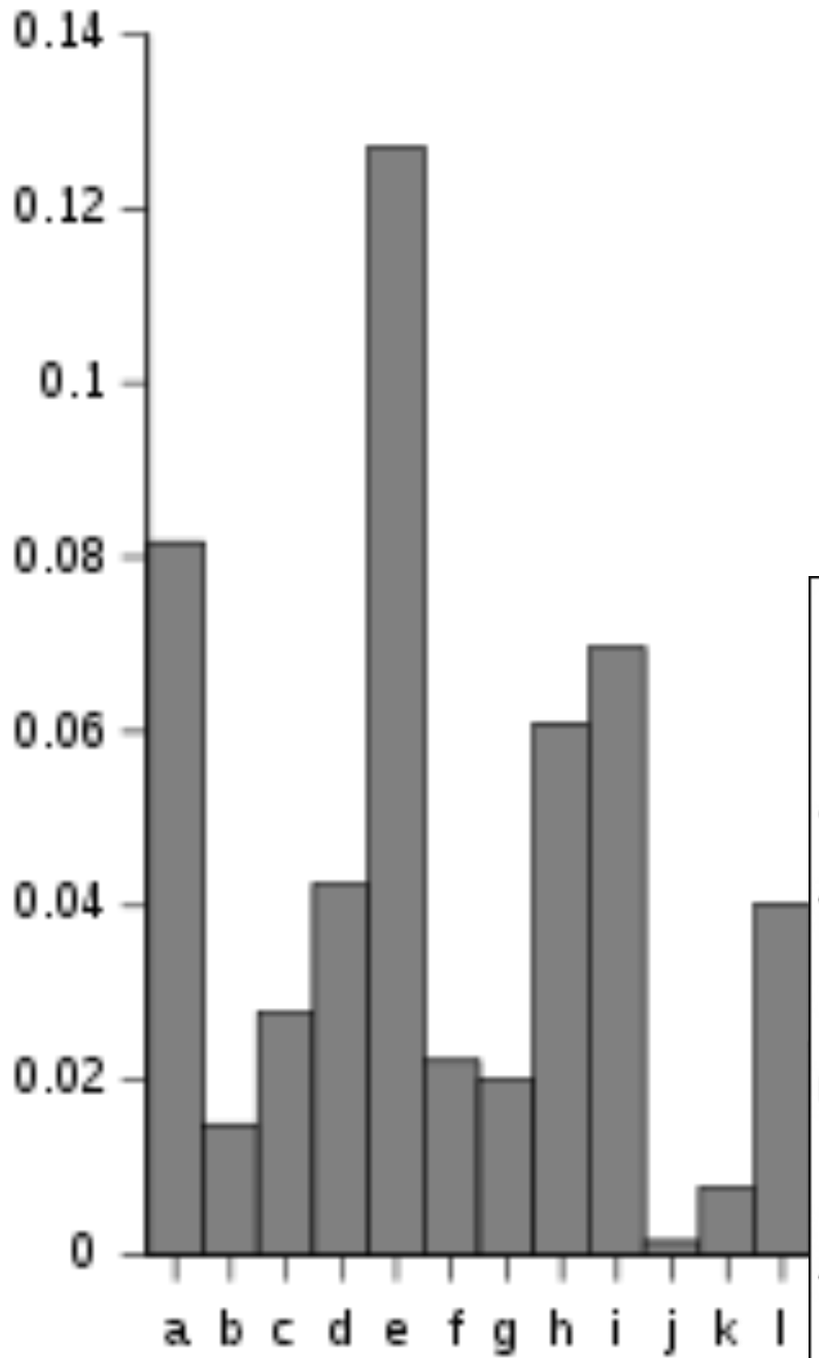
x	π(x)
A	Z
B	U
C	A
D	Y
E	R
F	E
G	X
H	B
I	D
J	C
K	M
L	Q
M	H
N	T
O	I
P	S
Q	V
R	N
S	P
T	K
U	O
V	F
W	G
X	W
Y	L
Z	J

How many keys?

$26! \approx 2^{88}$

9 million years to try all keys at rate of 1 trillion/sec

Cryptanalysis of Substitution Cipher



CELEBRITY CIPHER

by Luis Campos

Celebrity Cipher cryptograms are created from quotations by famous people, past and present. Each letter in the cipher stands for another.

“ U P X E G T H W Z H F X Y L F H O S L N P F X . H M

T P J S X E P O X V P G A V G P O S L E E B X X O A

P M L N P F X , T P J ’ C X Z P W E E B X V B P Z X

E B H O S . ” — V . W . Y X G V H O

Previous Solution: “Time is the cruelest teacher; first she gives the test, then teaches the lesson.” — Leonard Bernstein

TODAY'S CLUE: ſ ʃɹənbə N

Quick recall: Bitwise-XOR operation

We will use bit-wise XOR:

$$\begin{array}{r} 0101 \\ \oplus\ 1100 \\ \hline 1001 \end{array}$$

<u>Some Properties:</u>

- $X \oplus Y = Y \oplus X$
- $X \oplus X = 000\ldots0$
- $X \oplus Y \oplus X = Y$

Cipher Example: One-Time Pad

Key K: Bitstring of length L

Plaintext M: Bitstring of length L

Encrypt(K,M): Output K⊕M

Decrypt(K,C): Output K⊕C

Example:

$$\begin{array}{r} 0101 \\ \oplus\ 1100 \\ \hline 1001 \end{array}$$

Correctly decrypts because

$$K \oplus C = K \oplus (K \oplus m) = (K \oplus K) \oplus m = m$$

Q: Is the one-time pad secure?

Bigger Q: What does “secure” even mean?

Evaluating Security of Crypto

Kerckhoff's Principle: Assume adversary knows your algorithms and implementation. The only thing it doesn't know is the key.

1. Quantify adversary goals
   Learn something about plaintext? Spoof a message?
2. Quantify adversary capabilities
   View ciphertexts? Probe system with chosen inputs?
3. Quantify computational resources available to adversary
   Compute cycles? Memory?

International cyber crime ring smashed after more than $530 million stolen

By **Ben Westcott**, CNN

Updated 2:09 AM ET, Thu February 8, 2018