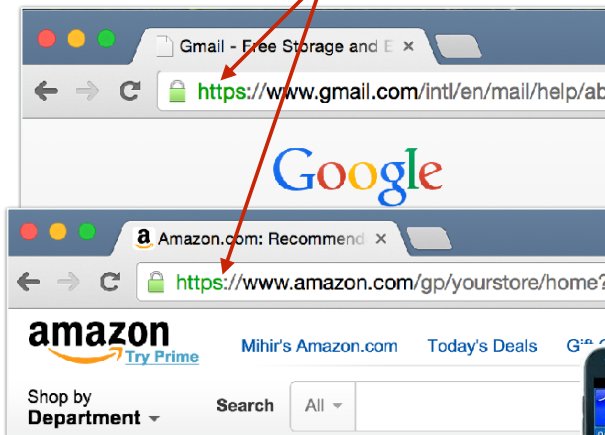


TLS/SSL



Username and password are sent over TLS/SSL

Credit-card number is sent over TLS/SSL

11,748 Android apps use cryptography.
10,327 of them get it wrong [EBFK13].



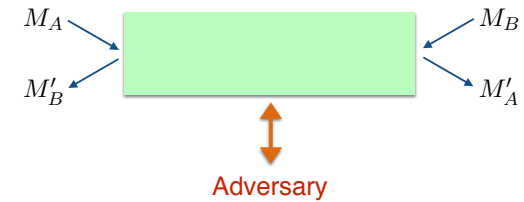
42

Mihir Bellare, UCSD

TLS/SSL aims to provide a **secure channel**

Client Alice

Server Bob



Privacy: Adversary does not learn anything about M_A, M_B

Authenticity: $M'_A = M_A$ and $M'_B = M_B$

Identity: Alice is really "Alice" and Bob is really "Bob"

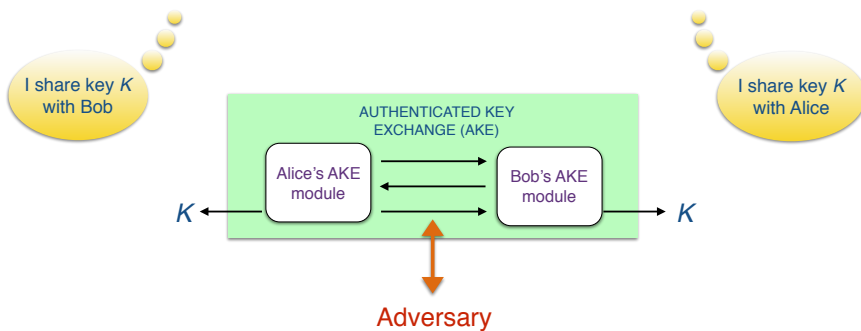
43

Mihir Bellare, UCSD

The cryptographic core of TLS/SSL

Client Alice

Server Bob



K is a fresh, authentic session key
Adversary cannot influence or know K

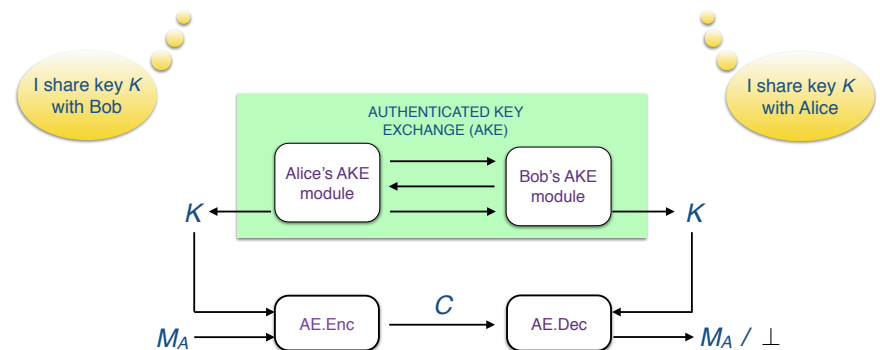
44

Mihir Bellare, UCSD

The cryptographic core of TLS/SSL

Client Alice

Server Bob

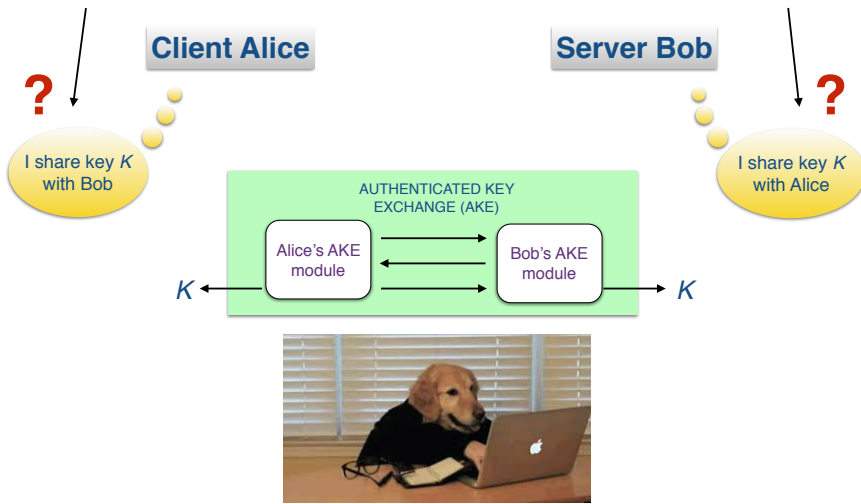


AE: Authenticated Encryption Scheme
C: Ciphertext
 \perp : REJECT

45

Mihir Bellare, UCSD

The question of identity: Who are "Alice" and "Bob"?



46

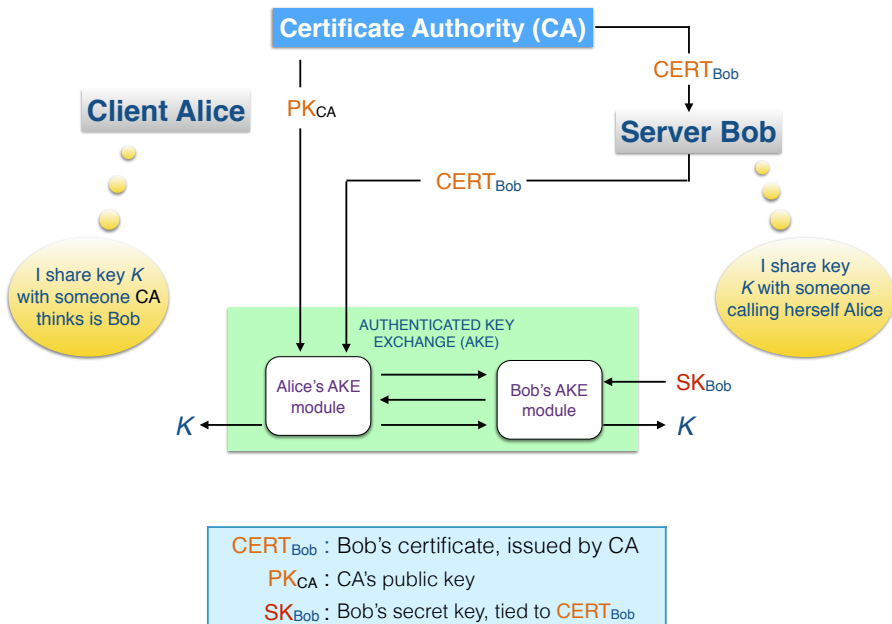
Mihir Bellare, UCSD

Who is "Bob"?



47

Mihir Bellare, UCSD



48

Mihir Bellare, UCSD

Certificate authorities

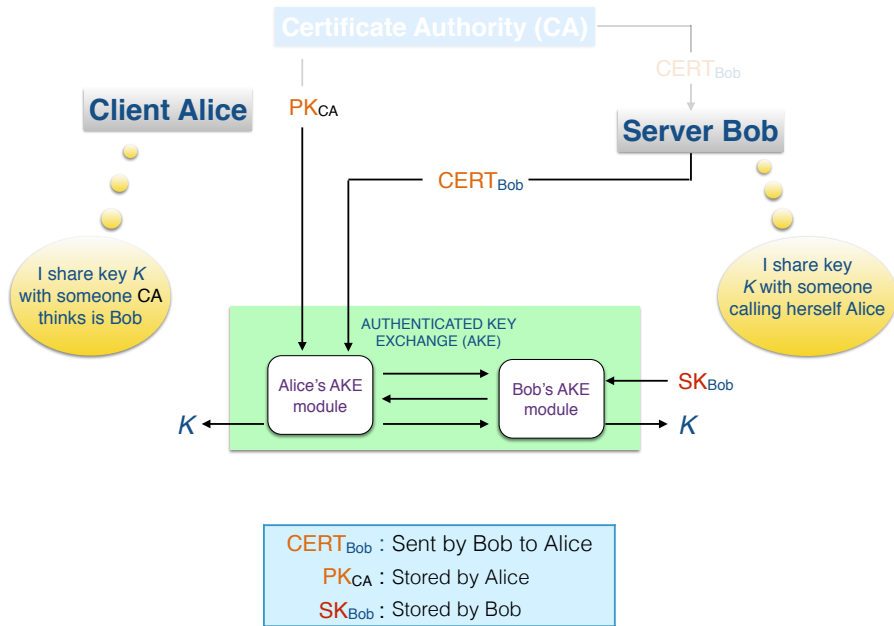
Rank	Issuer	Usage	market share
1.	Comodo	6.6%	33.6%
2.	Symantec Group	6.5%	33.2%
3.	Go Daddy Group	2.6%	13.2%
4.	GlobalSign	2.2%	11.3%
5.	DigiCert	0.6%	2.9%

As of February 2015

CA NAME	RATING
COMODO	★★★★★ (171 Reviews)
DigiCert	★★★★★ (1026 Reviews)
Entrust	★★★★★ (802 Reviews)
GeoTrust	★★★★★ (104 Reviews)
GlobalSign	★★★★★ (185 Reviews)
GoDaddy	★★★★★ (98 Reviews)
Network Solutions	★★★★★ (12 Reviews)
SSL.com	★★★★★ (44 Reviews)
StartCOM	★★★★★ (330 Reviews)
swissign	★★★★★ (4 Reviews)

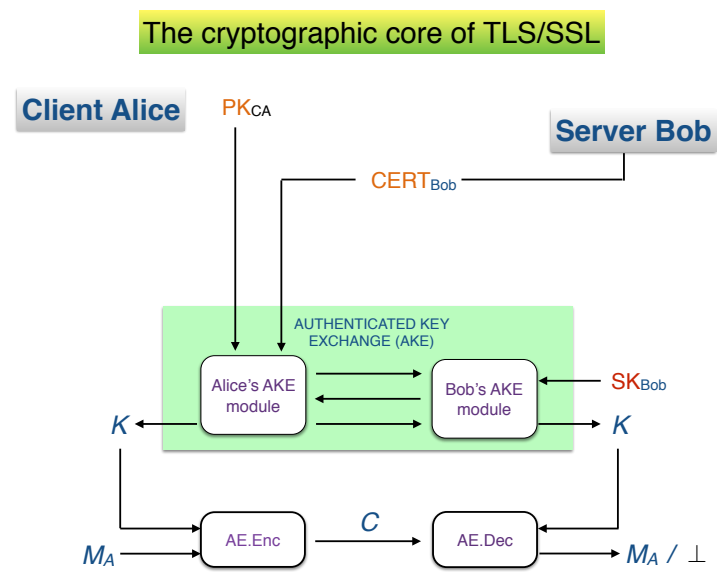
49

Mihir Bellare, UCSD



50

Mihir Bellare, UCSD

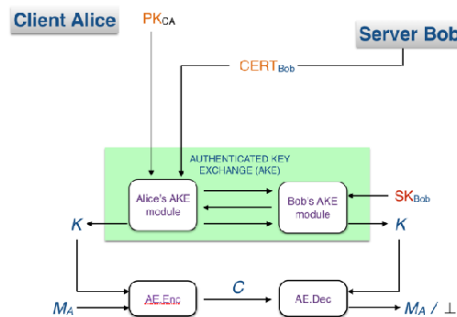


51

Mihir Bellare, UCSD

But who is "Alice?"

	AliceWonder@wonderland
	AliceWaters@chezpanisse
	AliceWalker@colorpurple
	AlicePoker@saloon



Default TLS/SSL provides **unilateral authentication**: Bob authenticates himself to Alice but not vice versa.

Alice does not typically have a certificate.

Alice will typically authenticate herself to Bob with username and password over the TLS/SSL channel itself.

52

Mihir Bellare, UCSD

TLS/SSL Vulnerabilities

POODLE vulnerability hastens the death of SSL 3.0

By James Sanders October

FREAK Attacks SSL/TLS Security, Putting Apple, Android Users at Risk

By Sean Michael Kerner | Posted 2015-03-04 | Email | Print



Apple's Safari and Google Android browsers are at risk from the newly discovered security encryption flaw known as Factoring attack on RSA-EXPORT Keys, or FREAK.

Heartbleed: 'Secure' internet wasn't safe

Security researchers have uncovered a fatal flaw in a key safety feature for surfing the Web -- the one that keeps your email, banking, shopping, passwords and communications private.

53

Mihir Bellare, UCSD

TLS/SSL Vulnerabilities

Vulnerability	crypto	Implementation/ Usage
FREAK	x	
Re-negotiation	x	
Version Rollback		x
BEAST	x	
Padding Oracle	x	
Lucky 13	x	
Poodle	x	x
Heartbleed		x
RC4	x	
AllYourSSLsAreBelongToUs		x

Many different TLS/SSL Implementations:
OpenSSL, GnuTLS, cryptlib, JSSE, RSA
BSafe, SChannel, ...

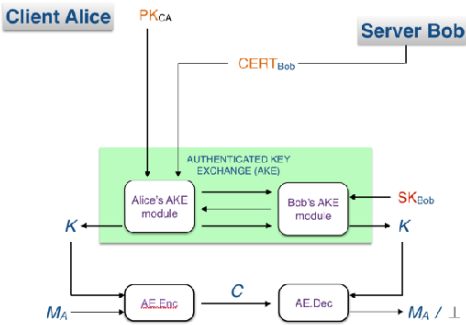
Issues: Cipher suites, re-negotiation, side-channels, buffer overflows, bad randomness, ...

Lots of **bad crypto** in TLS/SSL, often for historic and legacy reasons.



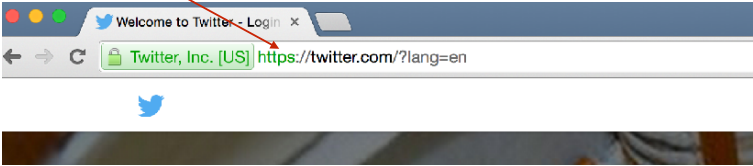
Get it right!

The cryptographic core of a secure channel



Summary, take away

TLS/SSL: Appreciate that there is a ton going on every time you access a website!



Providing a well-designed and analyzed cryptographic core is a central problem for us to address.