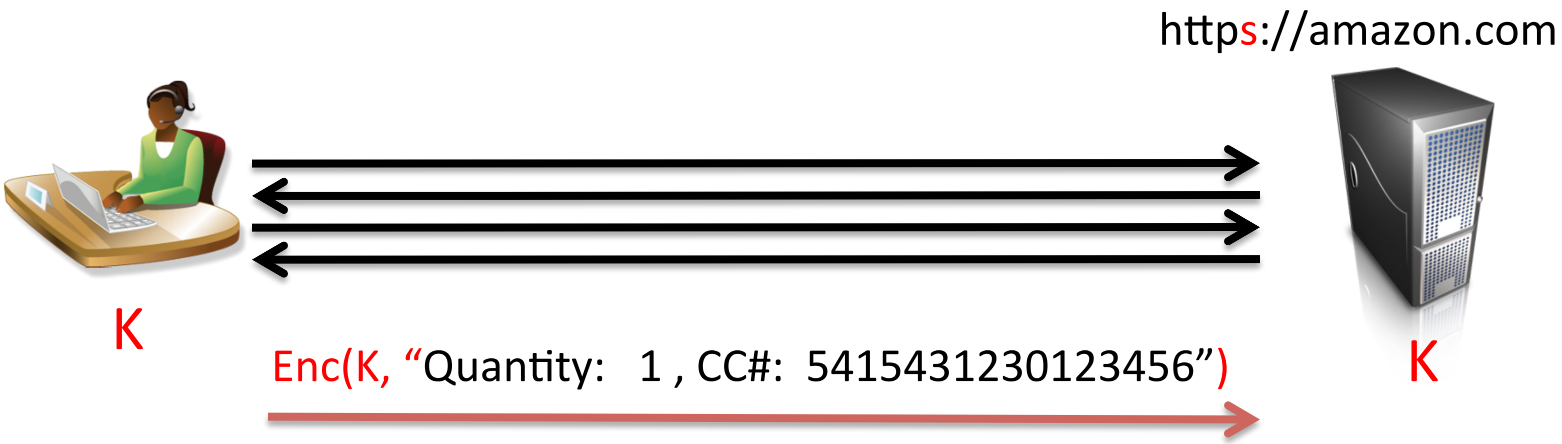
An example: On-line shopping with TLS



https://amazon.com

K

Enc(K, “Quantity: 1 , CC#: 5415431230123456”)

K

Step 1:
Key exchange
protocol to
share secret K

Step 2:
Send data via
secure
channel

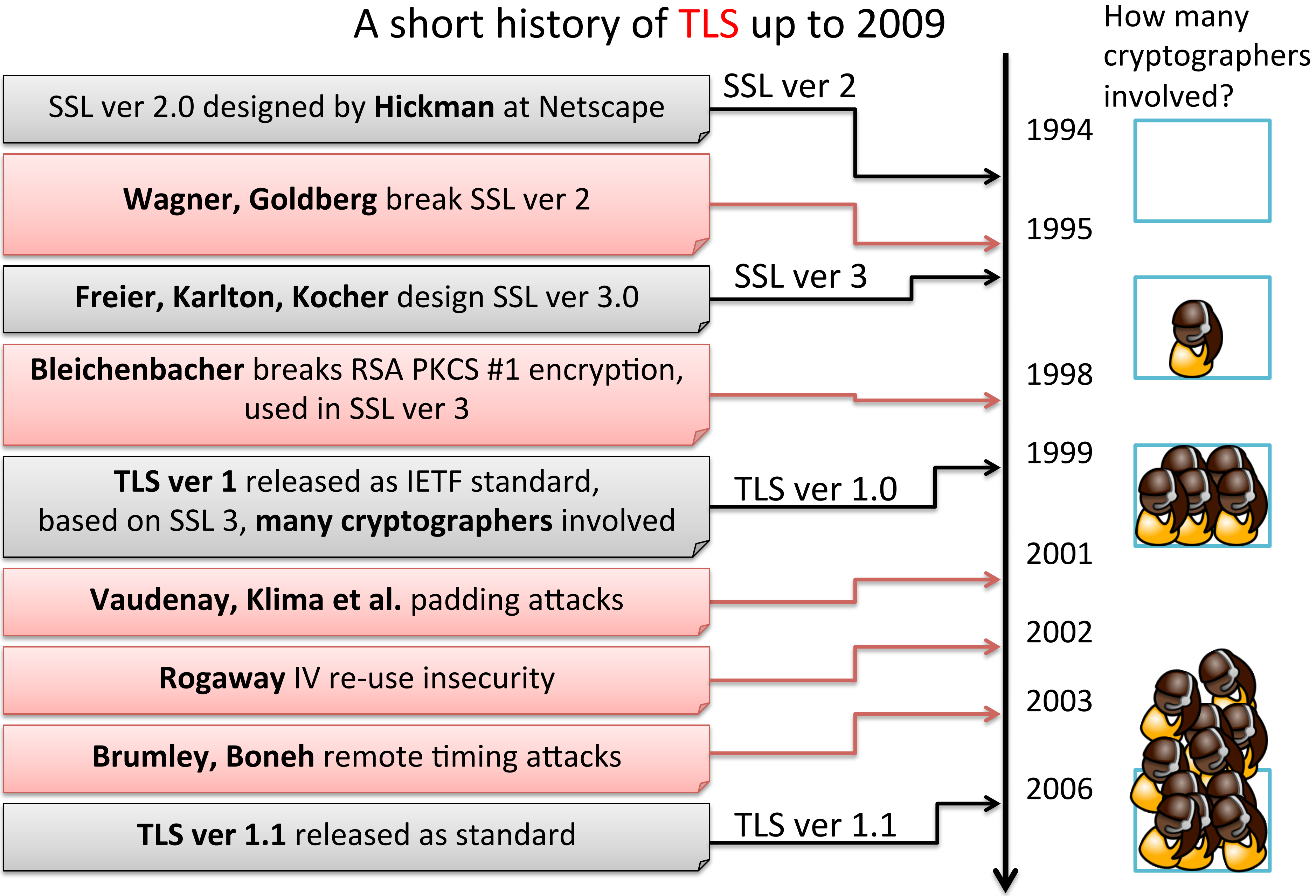
TLS uses many cryptographic primitives:

key exchange: hash functions, digital signatures, public key encryption

secure channel: symmetric encryption, message authentication

Mechanisms to resist replay attacks, man-in-the-middle attacks, truncation attacks, etc…

A short history of TLS up to 2009



SSL ver 2.0 designed by **Hickman** at Netscape

Wagner, Goldberg break SSL ver 2

Freier, Karlton, Kocher design SSL ver 3.0

Bleichenbacher breaks RSA PKCS #1 encryption, used in SSL ver 3

TLS ver 1 released as IETF standard, based on SSL 3, **many cryptographers** involved

Vaudenay, Klima et al. padding attacks

Rogaway IV re-use insecurity

Brumley, Boneh remote timing attacks

TLS ver 1.1 released as standard

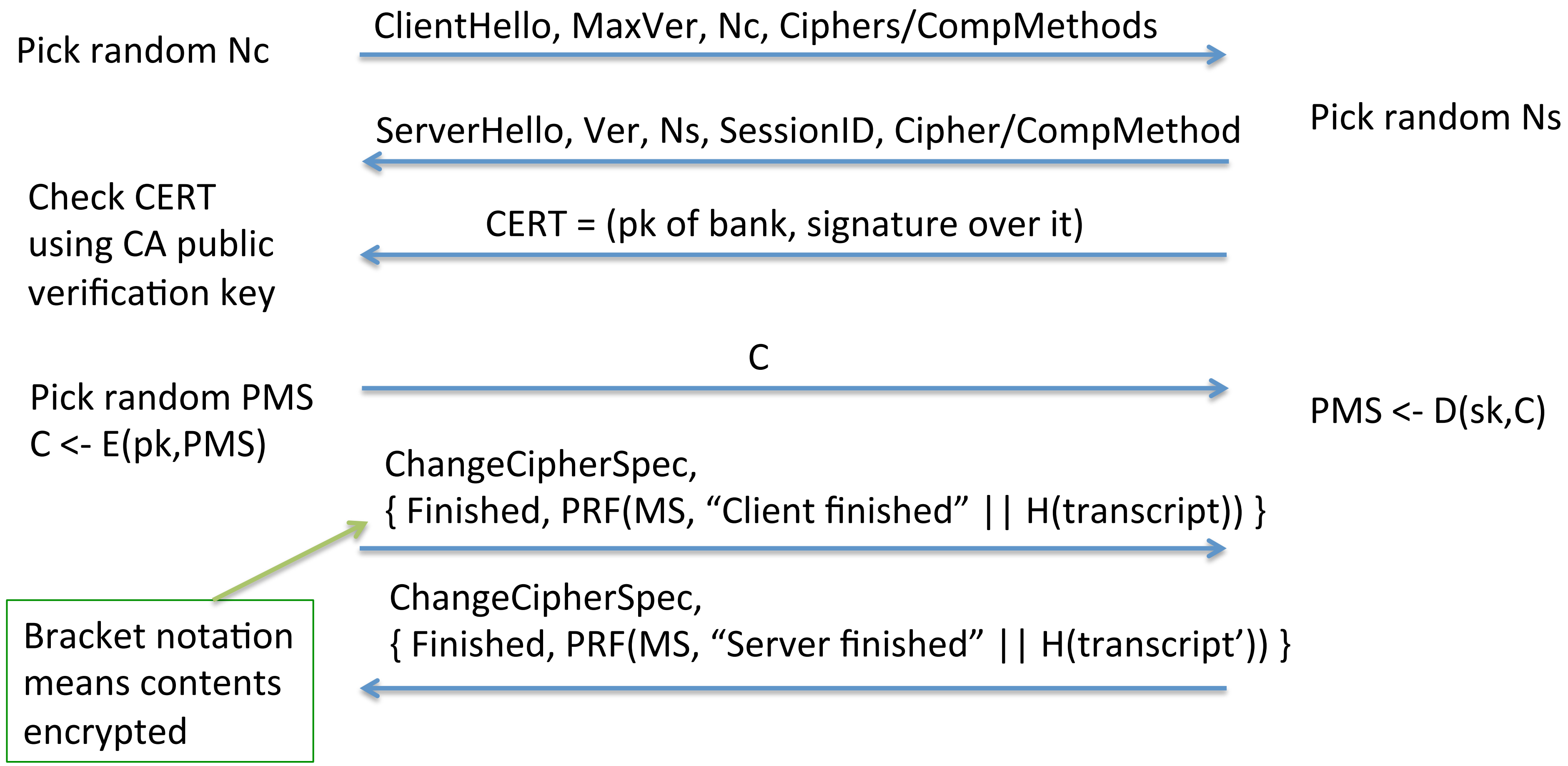
⋮

(more attacks and fixes)

Bank customer

TLS handshake for RSA transport

Bank



Pick random Nc

ClientHello, MaxVer, Nc, Ciphers/CompMethods

ServerHello, Ver, Ns, SessionID, Cipher/CompMethod

Pick random Ns

Check CERT using CA public verification key

CERT = (pk of bank, signature over it)

Pick random PMS
C <- E(pk,PMS)

C

PMS <- D(sk,C)

ChangeCipherSpec,
{ Finished, PRF(MS, “Client finished” || H(transcript)) }

Bracket notation means contents encrypted

ChangeCipherSpec,
{ Finished, PRF(MS, “Server finished” || H(transcript’)) }

MS <- PRF(PMS, “master secret” || Nc || Ns)

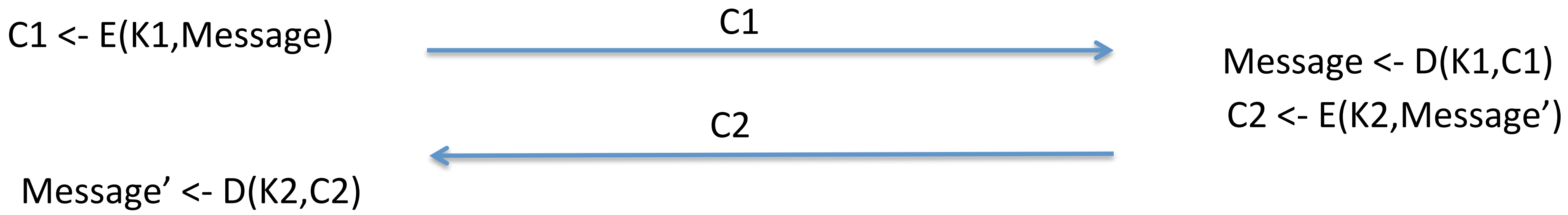
Bank customer

TLS Record layer

Bank

MS <- PRF(PS, “master secret” || Nc || Ns)

K1,K2 <- PRF(MS, “key expansion” || Ns || Nc)



C1 <- E(K1,Message)

C1

Message <- D(K1,C1)

C2 <- E(K2,Message’)

C2

Message’ <- D(K2,C2)