An example: On-line shopping with TLS

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

TLS ver 1.0

1994
1995
1998
1999
2001
2002
2003
2006

(more attacks and fixes)

How many cryptographers involved?
## TLS handshake for RSA transport

<table>
<thead>
<tr>
<th>Step</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pick random Nc</td>
</tr>
<tr>
<td>Check CERT using CA public verification key</td>
</tr>
<tr>
<td>Pick random PMS C &lt;- E(pk,PMS)</td>
</tr>
</tbody>
</table>

### Messages:

- **ClientHello, MaxVer, Nc, Ciphers/CompMethods**
- **ServerHello, Ver, Ns, SessionID, Cipher/CompMethod**
- **CERT = (pk of bank, signature over it)**
- **C**
- **ChangeCipherSpec,**
  - `Finished, PRF(MS, “Client finished” || H(transcript))`
- **ChangeCipherSpec,**
  - `Finished, PRF(MS, “Server finished” || H(transcript'))`
- **MS <- PRF(PMS, “master secret” || Nc || Ns )**

### Notes:
- Bracket notation means contents encrypted
**TLS Record layer**

Bank customer  

Bank

---

\[
MS \gets \text{PRF}(PS, \text{“master secret”} \ || \ Nc \ || \ Ns )
\]

\[
K1,K2 \gets \text{PRF}(MS, \text{“key expansion”} \ || \ Ns \ || \ Nc )
\]

\[
C1 \gets \text{E}(K1, \text{Message})
\]

\[
\text{Message} \gets \text{D}(K1,C1)
\]

\[
C2 \gets \text{E}(K2, \text{Message’})
\]

\[
\text{Message’} \gets \text{D}(K2,C2)
\]