Heartbleed - New Server
Heartbleed - New Client
SSLv3, SSLv2, BEA SSL, CRIME, Heartbleed

Attacks on Ciphersuites SSL

Send it back
Heartbreak was a bug.
- browser does not check.

and/or

- support features to turn off bannering

- cert changes

especially
Sign it with initial and plan

Scheme to be graphed first

Movable root cut (supplied)

Close menu

Part cut in root key

Groove

Cut out

Cut out

Groove
Read change response (gen 2)
Drawing in each
Question:
Le Petit 6 sounds in to which
Smartenko -
$ L_{hash\ map} \rightarrow msg\ with\ code$ 

$\text{HMAC is used in both cases}$

$T_0 \rightarrow \text{time bound one time password}$

$T_{0,0} \rightarrow \text{hash bound one time password}$

Authentication via one time password
\text{Hash}(\text{k} \oplus \text{pad}) \parallel \text{m}

\text{Hash}(\text{k} \oplus \text{opad}) \parallel \text{m}

\text{Pad} = 0x \ 363636 \ldots

\text{opad} = 0x \ 5c5c5c \ldots

\text{count}

\text{Key}

\text{Hash} (k, m)
A country needs a default mode. A country needs default mode. Yubiker -> many more

work time

↑

top = replace country with time
Key
AES
Count
output = 10 || E(key)

Key
AES
IV
10
easy to verify

- software on disk in simplest key

- no method to exchange key

- key in the physical device

- enhance security

stolen/lost

why the fees?
I/O

CPU

RAM

Keys

Keys & Coordinates

File - Courses (have embedded pairs)

User Interface
Example → DoD CAC card

Common Access Card
Sign graphics (can secure smoke)

Encrypted password (bells)

Key exchange

Authentication (PKI簽章)

What does it do