

MIT OpenCourseWare  
<http://ocw.mit.edu>

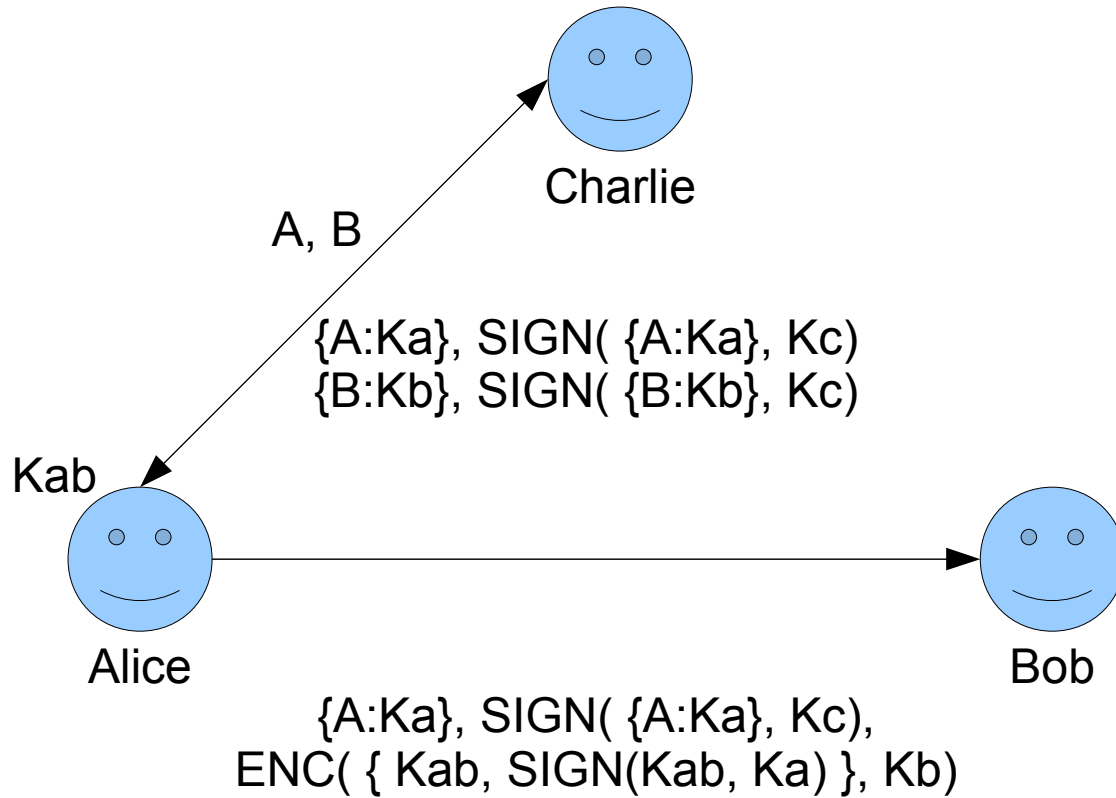
6.033 Computer System Engineering  
Spring 2009

For information about citing these materials or our Terms of Use, visit: <http://ocw.mit.edu/terms>.

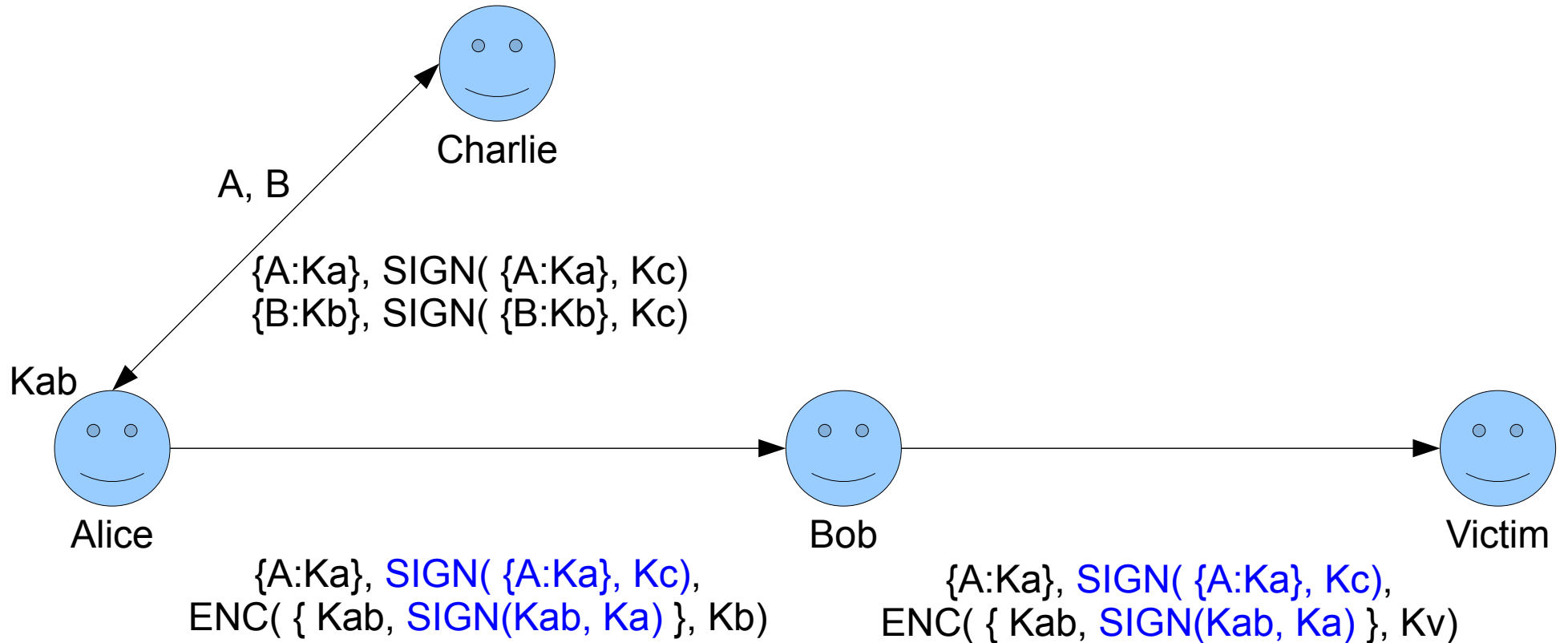
6.033 Lecture 24  
Protocols and Authorization

Nickolai Zeldovich

# Denning-Sacco Protocol



# Denning-Sacco Protocol



# Denning-Sacco Protocol

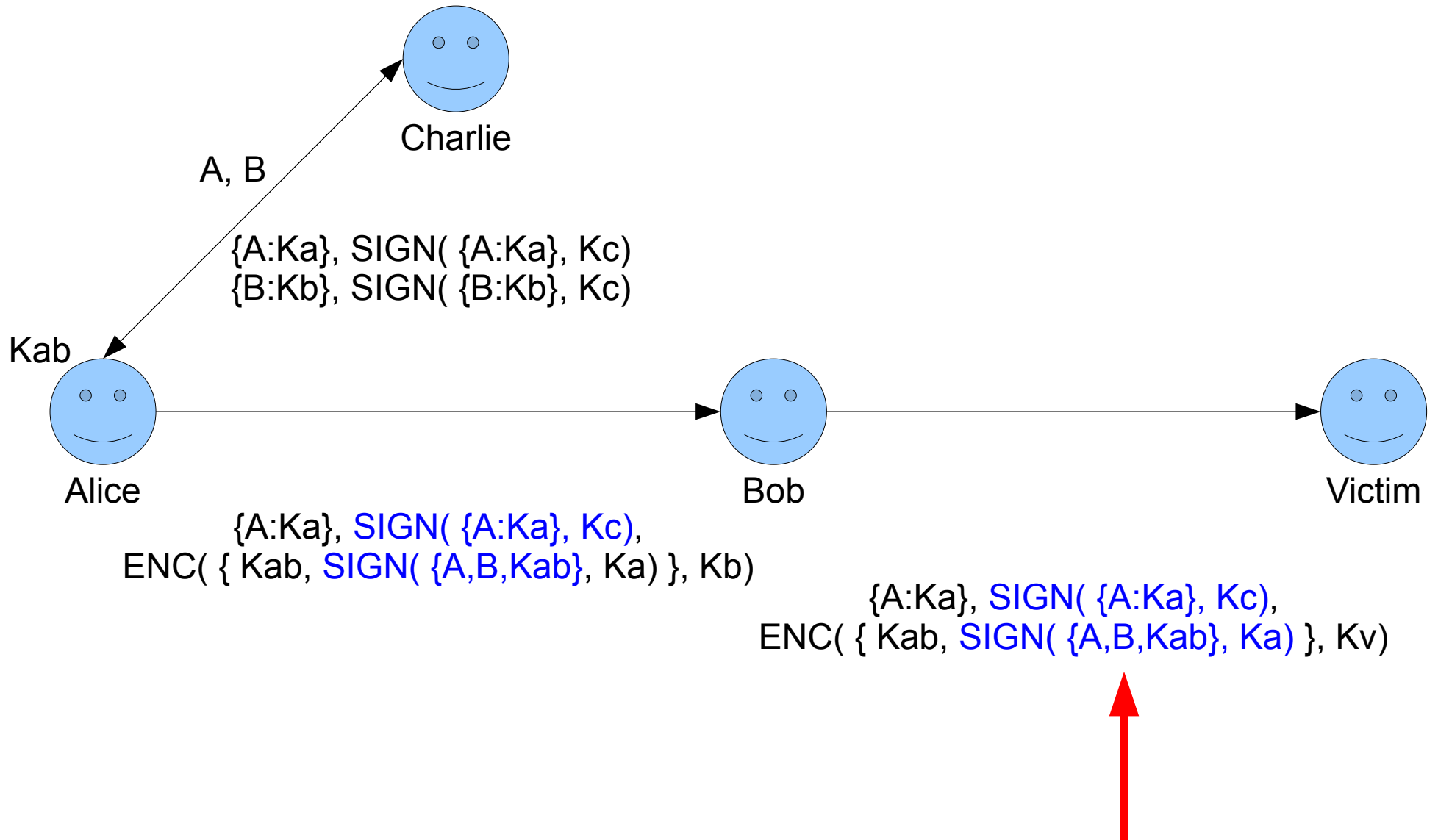


Diagram of SSL handshake with two-way authentication removed due to copyright restrictions. See the [Wikipedia page](#) instead.

# How confidential is traffic in this lecture room?

- `sudo tcpdump -s 0 -Ai en1`
  - Complete trace of all packets on wireless network
  - You shouldn't do this
- 14:04:59.999646 IP HSI-KBW-091-089-230-121.hsi2.kabel-badenwuerttemberg.de.45843 > dhcp-18-111-20-195.dyn.mit.edu.39211: P 127234932:127234940(8) ack 4112680742 win 65429 <nop,nop,timestamp 6345692 18015400>

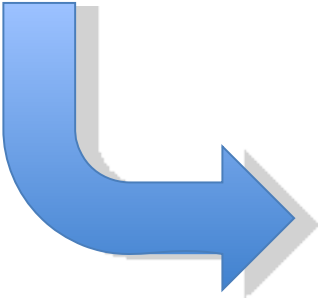
# Example Data Inside a Packet

```
GET /6.033/2007/wwwdocs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_5_6; en-us) AppleWebKit/525.27.1 (KHTML, like Gecko)
Referer: http://mit.edu/6.033/2008/wwwdocs/schedule.html
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png;q=0.8
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Connection: keep-alive
Host: mit.edu
```



# Example Data Inside a Packet

GET /6.033/2007/wwwdocs/ HTTP/1.1  
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10\_5\_6; en-us) AppleWebKit/525.27.1 (KHTML, like Gecko) Chrome/19.0.939.74 Safari/525.27.1  
Referer: http://mit.edu/6.033/2008/wwwdocs/schedule.html  
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png;q=0.8  
Accept-Language: en-us  
Accept-Encoding: gzip, deflate  
Connection: keep-alive  
Host: mit.edu



HTTP/1.1 200 OK  
Date: Wed, 29 Apr 2009 18:56:00 GMT  
Server: MIT Web Server Apache/1.3.26 Mark/1.5 (Unix) mod\_ssl/2.8.9 OpenSSL/0.9.7c  
Last-Modified: Fri, 25 May 2007 17:15:48 GMT  
ETag: "b884046-46a4-465719c4"  
Accept-Ranges: bytes  
Content-Length: 18084  
Connection: close  
Content-Type: text/html

<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">  
<html>  
<head>  
<title>6.033 / Spring 2007 / Welcome</title>  
...

# GMail is not encrypted by de

Passed in the clear:

- Contacts lists
- Calendar events

Gzipped text:

- Inbox entries
- Mail messages

```
["112677a23fed4887",0,0,"12:58 pm","\u003cspan id\u003d\"_upro_ \"\>Richard Stallman\u003c/span\u003e","\&nbsp;","\[csail- related] big brother--trade charlie cards. 13:45 Tuesday at 381","I have a charlie card with zero value current on on it which I used for a couple of &hellip;",[],"", "112677a23fed4887",0,"Mon May 7 2007_12: PM",0,"",0,0,1]
```

**Hint: Change <http://> to <https://>**

# Facebook is Plaintext

(as is AIM, Google Docs, iChat, etc...)

```
{"name": "XX XXXX",  
"firstName": "XX",  
"thumbSrc": "XXX.jpg",  
"status": "says a man should  
always dress for the job he  
wants. So why am I dressed up  
like a pirate in this restaurant?  
It's all because some hacker  
stole my identity, now I sit  
here every evening serving  
chowder and iced tea.  
Should've gone to  
FreeCreditReport.com, I  
could've seen this coming at  
me like an atom bomb. They  
monitor your credit and send  
you e-mail alerts, so you don't  
end up selling fish to tourists in  
t-shirts.",  
"statusTime":1240674216,  
"statusTimeRel":"on Saturday",  
"enableVC":false}
```

Screenshot of Facebook page removed  
due to copyright restrictions.

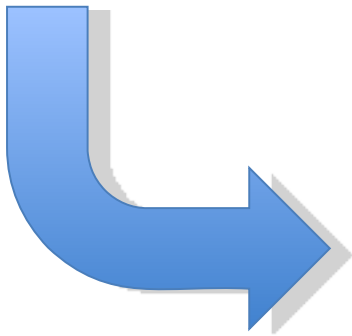
# Authentication Cookies

HTTP/1.1 200 OK

Set-Cookie: **CAL=XXXXXXXXXXXX**;Domain=**www.google.com**;Path=/calendar;  
Expires=Tue, 19-May-2009 18:23:37 GMT

Cache-Control: no-cache, no-store, max-age=0, must-revalidate

Pragma: no-cache



Screenshot of Google Calendar removed  
due to copyright restrictions.

# Authentication Cookies

HTTP/1.1 200 OK

Date: Mon, 04 May 2009 18:20:10 GMT

...

Set-Cookie: \_twitter\_sess=XXXXXXXXXXXXX; domain=**.twitter.com**; path=/

HTTP/1.1 200 OK

Date: Mon, 04 May 2009 18:06:24 GMT

...

Set-Cookie: xs=XXXXXXXXXXXXX; path=/; domain=**.facebook.com**;

HTTP/1.1 200 OK

Date: Mon, 04 May 2009 18:19:19 GMT

...

Set-Cookie: itsessionid=XXXXXXXXXXXXX; path=/;  
domain=**.analytics.yahoo.com**

etc etc etc