

L24: Secure channels

Nickolai Zeldovich
6.033 Spring 2011

Network insecurity

```
# tcpdump -A -s 2272 -i mon0
11:53:41.281771 2462 MHz 11g -26dB signal antenna 15 [bit 14]
  CF +QoS IP 128.31.33.180.41899 > 74.125.226.180.80: Flags
  [P.], seq 490544447:490545563, ack 2165662404, win 501,
  options [nop,nop,TS val 701636 ecr 3105280684], length 1116
...
GET /search?hl=en&source=hp&q=mit+150&... HTTP/1.1
Host: www.google.com
Connection: keep-alive
Referer: http://www.google.com/
User-Agent: Mozilla/5.0 (X11; CrOS i686 0.0.0) ...
Cookie: NID=45=0N-XmK6HCc6gnbx-DAQck2-IBwUK8JV-79rK3iFzK08pL...
...
```

Diffie-Hellman key exchange

Alice

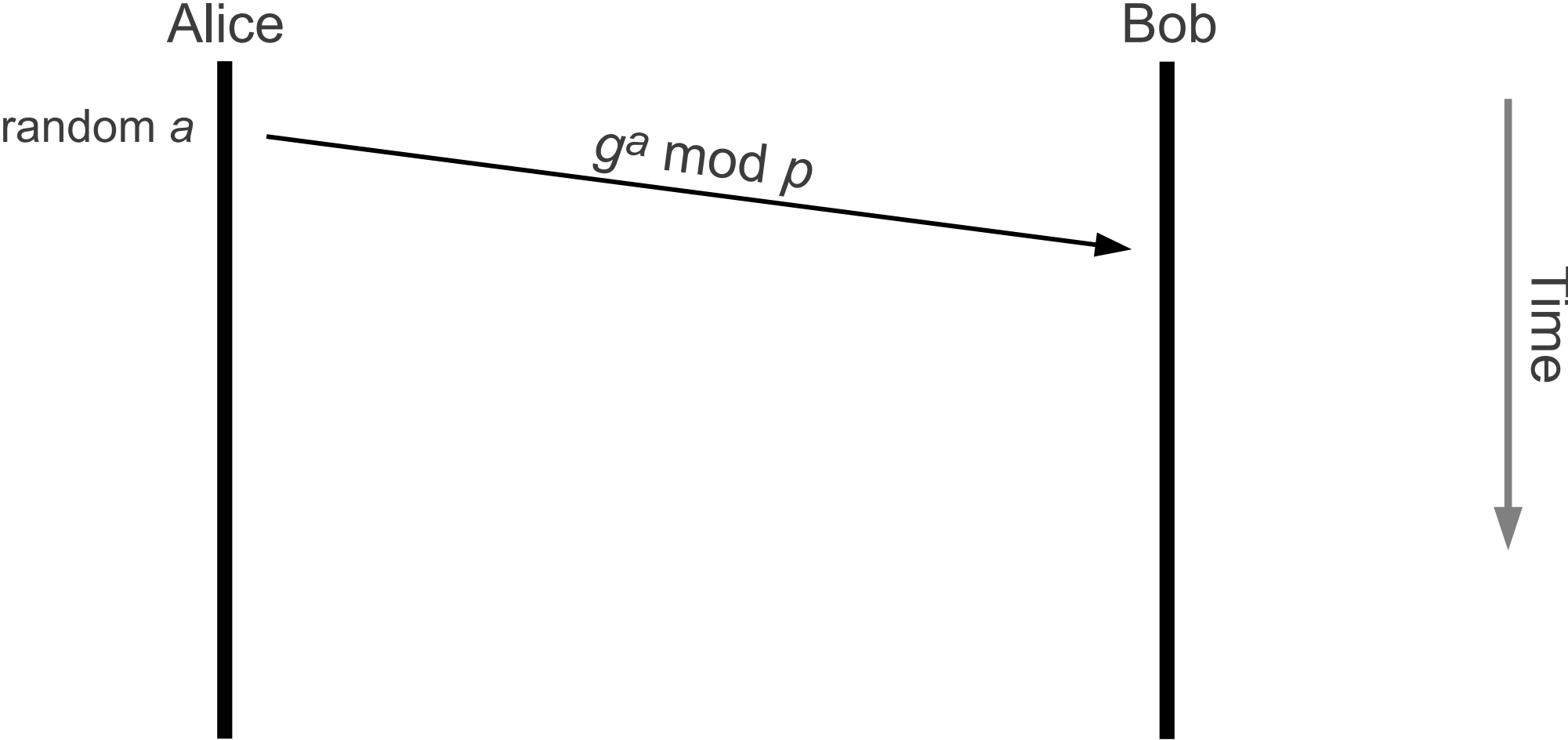


Bob



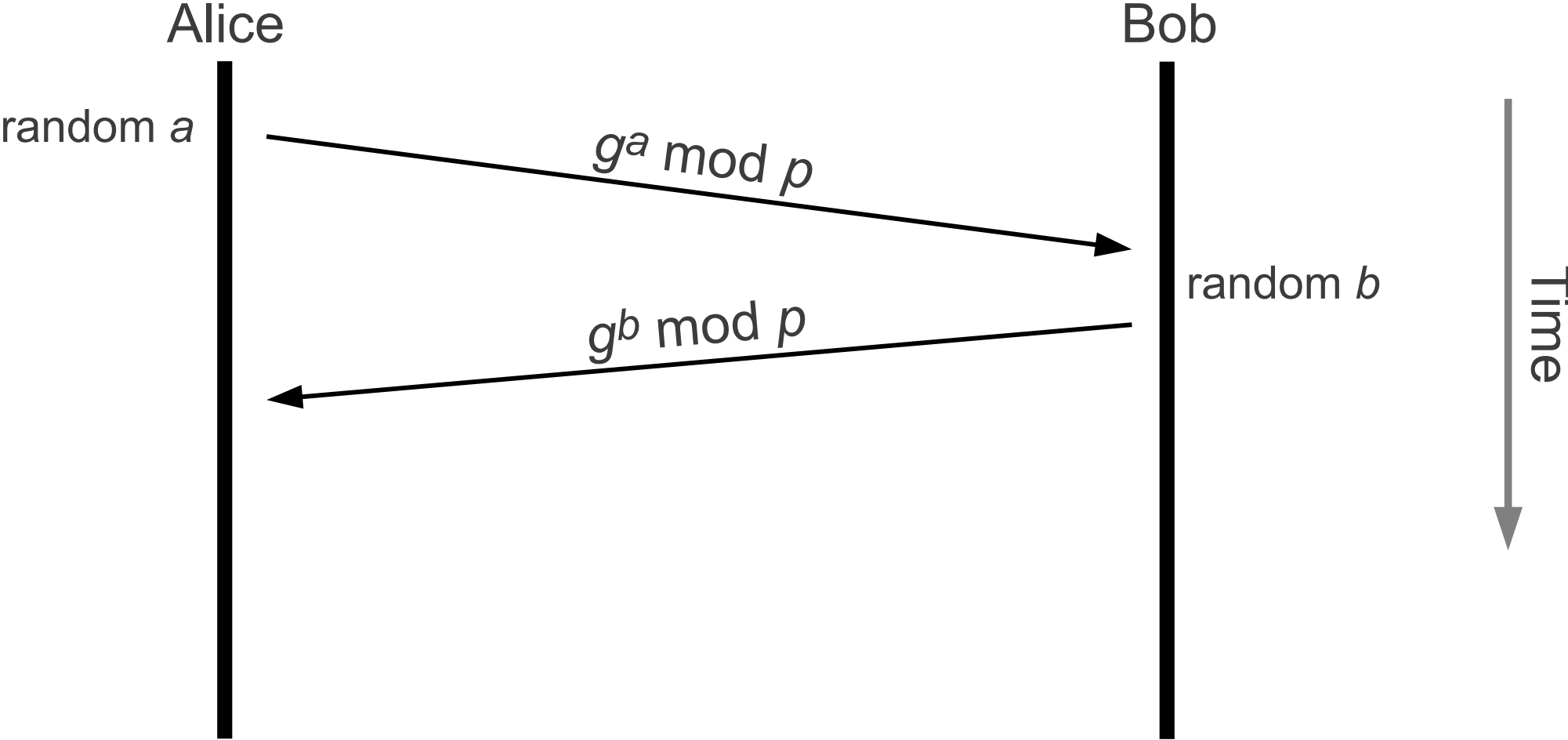
Common parameters: prime p , generator g

Diffie-Hellman key exchange



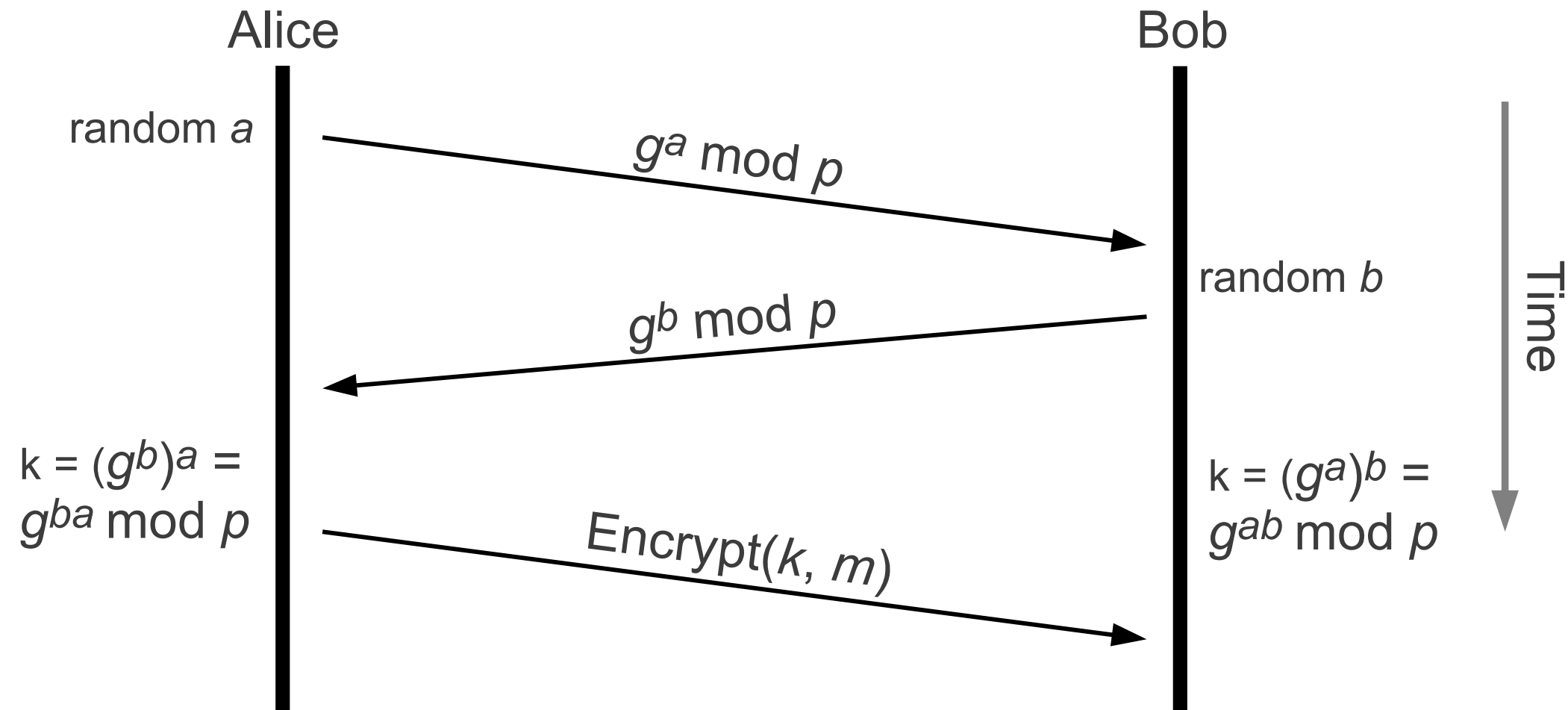
Common parameters: prime p , generator g

Diffie-Hellman key exchange



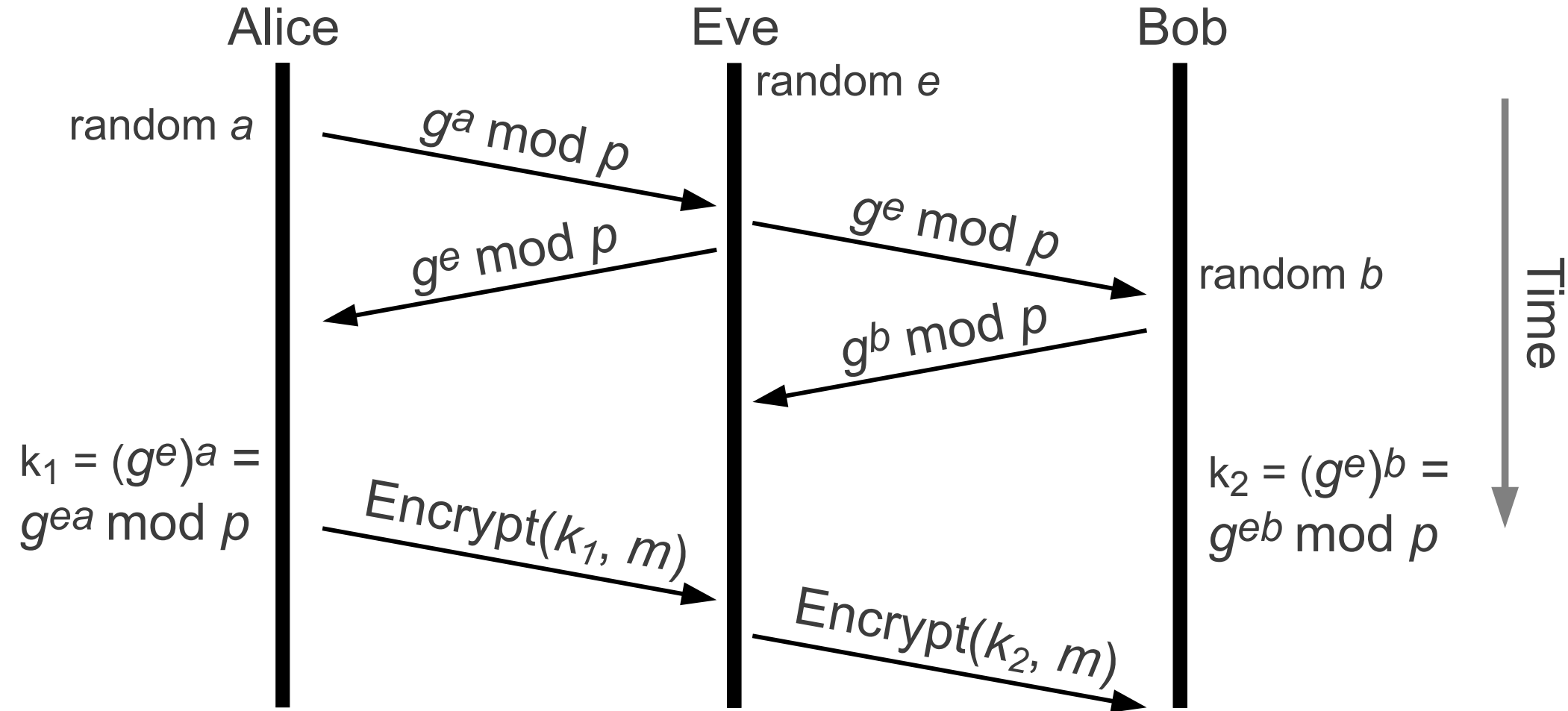
Common parameters: prime p , generator g

Diffie-Hellman key exchange



Common parameters: prime p , generator g

Man-in-the-middle (MITM) attack



Common parameters: prime p , generator g

Certificate authority mistakes

- 2001: Verisign issues certificate attesting that some public key belongs to Microsoft Corp.
 - Key belonged to some individual, not MS
- 2011: Comodo issues certs for *mail.google.com*, *login.yahoo.com*, *login.skype.com*, *login.live.com*, *addons.mozilla.org*, ...
 - Key belonged to someone else (not clear who)