Cryptography and Internet Security

How mathematics makes it safe to shop on-line

John Lindsay Orr
University of Nebraska - Lincoln

http://www.math.unl.edu/~jorr/presentations

Goals

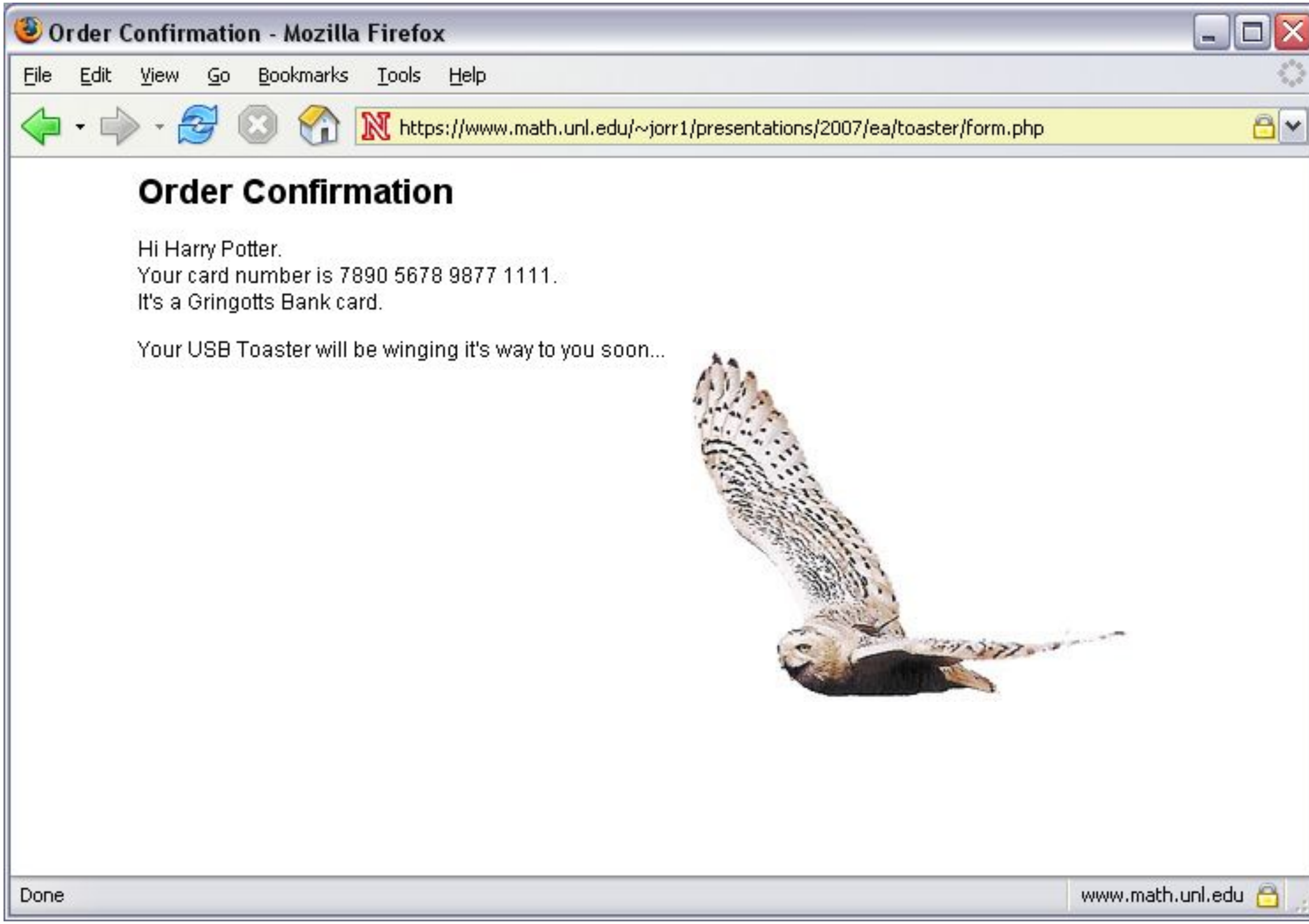
- Bad guys on the net: Why we need internet security
- Codes and ciphers: Julius Caesar and MI5
- The chicken and the egg: Asymmetric ciphers
- 525,600 minutes : Why asymmetric ciphers work
- The bad guys get smart: Man-in-the-middle attacks
- Digital signatures and certificate authorities
- Security ain’t safety: Phishing

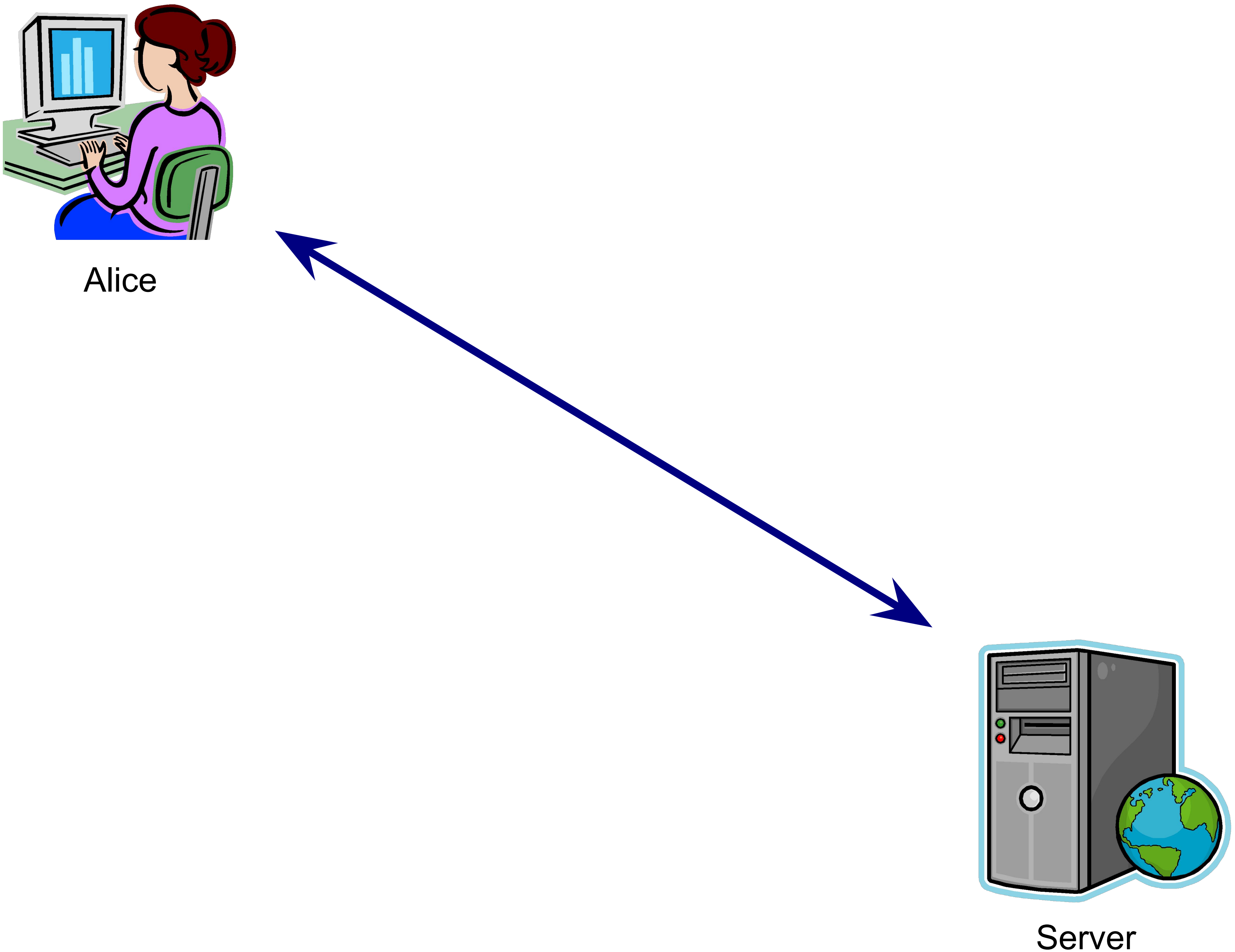
Bad Guys on the Net

Why we need internet security

Order your USB toaster here! - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.math.unl.edu/~jorr1/presentations/2007/ea/toaster/
The Amazing USB Toaster
Name: Harry Potter
Credit Card Number: 7890 5678 9877 1111
Credit Card Type: Gringotts Bank
Buy It Now!
Fresh on-the-go toast!
DigiPliance
USB Toaster
Single Slice USB Powered Toasting Computer Accessory
BIG OL'
FLAP ON EACH END
GOTCHA!
SALT
CLUB
MAKE-YOUR-OWN
Umbrella Kit
Done

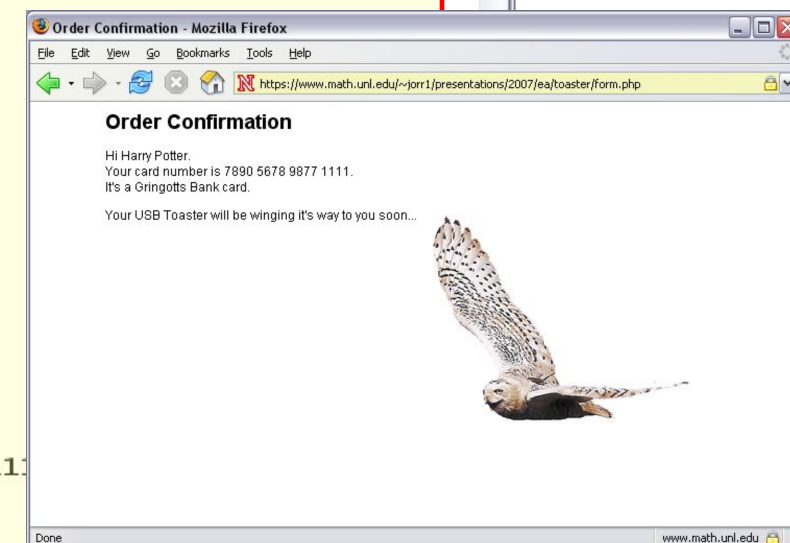
Order your USB toaster here! - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://www.math.unl.edu/~jorr1/presentations/2007/ea/toaster/
The Amazing USB Toaster
Name: Harry Potter
Credit Card Number: 7890 5678 9877 1111
Credit Card Type: Gringotts Bank
Buy It Now!
DigiPliance
USB Toaster
Single Slice USB Powered Toasting Computer Accessory
Fresh on-the-go toast!
BIG OL' FLAP ON EACH END
GOTCHA!
SALT CLUB
MAKE-YOUR-OWN Umbrella Kit
Done
www.math.unl.edu

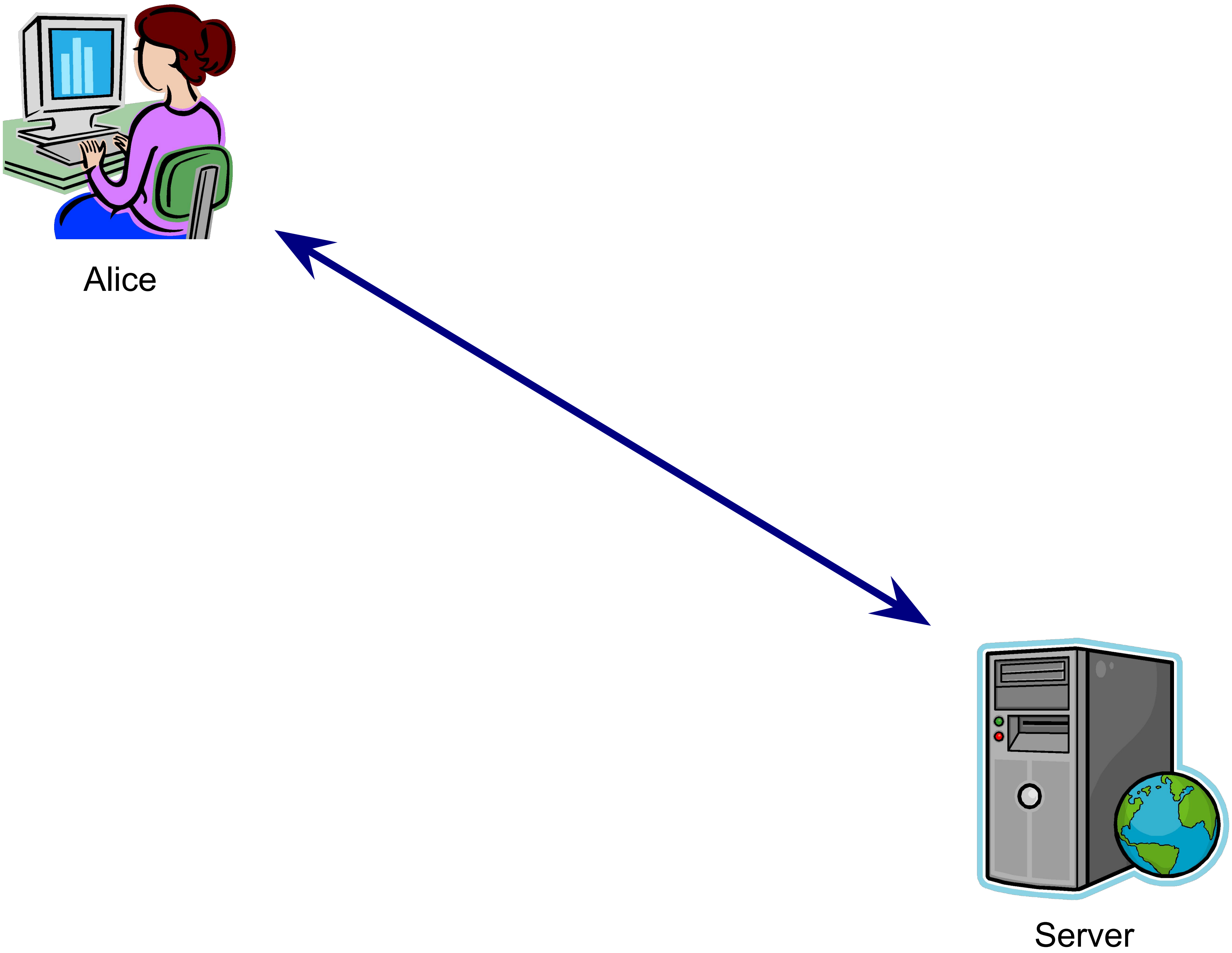

Order Confirmation - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://www.math.unl.edu/~jorr1/presentations/2007/ea/toaster/form.php
Order Confirmation
Hi Harry Potter.
Your card number is 7890 5678 9877 1111.
It's a Gringotts Bank card.
Your USB Toaster will be winging it's way to you soon...
Done
www.math.unl.edu


Alice
Server

math.unl.edu - PuTTY

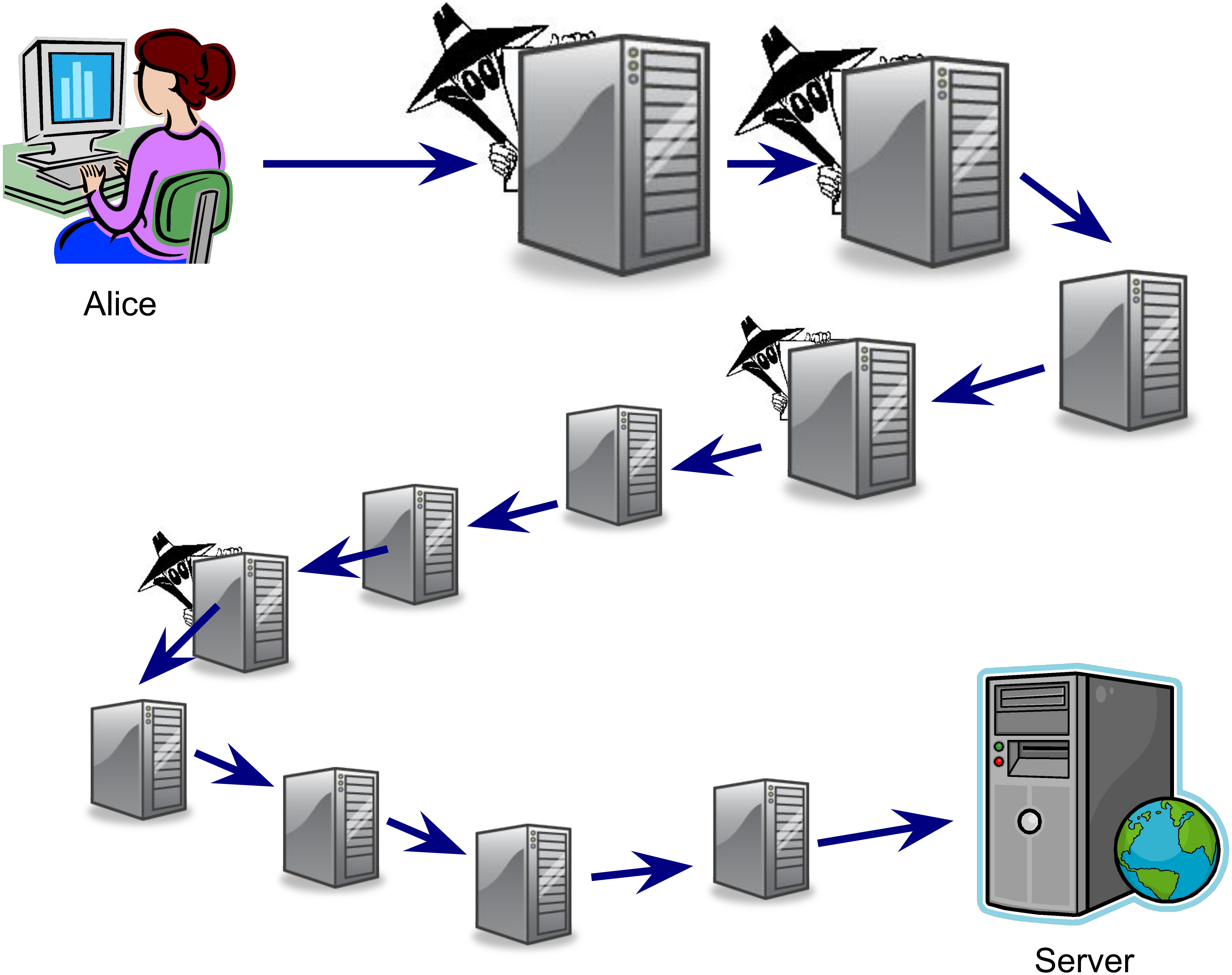
```
math> telnet www.math.unl.edu 80
Trying 129.93.180.31...
Connected to www.math.unl.edu.
Escape character is '^]'.
POST /~jorr1/presentations/2007/ea/toaster/form.php HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 62

name=Harry Potter&card=7890 5678 9877 1111&type=Gringotts Bank
HTTP/1.1 200 OK
Date: Mon, 26 Feb 2007 13:39:36 GMT
Server: Apache/2.0.52 (CentOS)
X-Powered-By: PHP/4.3.9
Content-Length: 379
Connection: close
Content-Type: text/html

<html>
  <head>
    <title>Order Confirmation</title>

    <style>
      @import URL("style.css");
    </style>
  </head>

  <body>

    <h1>Order Confirmation</h1>

    Hi Harry Potter.<br>
    Your card number is 7890 5678 9877 111
    It's a Gringotts Bank card.
    <p>
    Your USB Toaster will be winging it's way to you soon...
  </body>
</html>
Connection closed by foreign host.
math>
```




Alice
Server

C:\WINNT\system32\cmd.exe

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

H:\>pathping www.math.unl.edu

Tracing route to mobius.unl.edu [129.93.180.31]
over a maximum of 30 hops:
  0  fyb043000009.lancs.local [148.88.169.40]
  1  148.88.168.1
  2  cp10k-fy5i.rtr.lancs.ac.uk [148.88.255.93]
  3  bar7i-cp10k.rtr.lancs.ac.uk [148.88.255.18]
  4  194.81.46.1
  5  so-1-3-0.warr-sbr1.ja.net [146.97.42.177]
  6  so-0-2-0.read-sbr1.ja.net [146.97.33.109]
  7  lond-scr3.ja.net [146.97.33.142]
  8  po1-0.gn2-gw1.ja.net [146.97.35.98]
  9  janet.rt2.lon.uk.geant2.net [62.40.124.197]
 10  so-2-0-0.rt1.ams.nl.geant2.net [62.40.112.137]
 11  so-7-0-0.rt1.nyc.us.geant2.net [62.40.112.134]
 12  198.32.11.50
 13  so-0-0-0.0.rtr.wash.net.internet2.edu [64.57.28.11]
 14  64.57.28.12
 15  64.57.28.0
 16  iplsng-chinng.abilene.ucaid.edu [198.32.8.77]
 17  kscyng-iplsng.abilene.ucaid.edu [198.32.8.81]
 18  ks-2-p00.r.greatplains.net [164.113.238.194]
 19  ks-4-t2.r.greatplains.net [164.113.238.206]
 20  wsec6-fa-3-45.unl.edu [129.93.5.45]

Computing statistics for 500 seconds...

H:\>_
```


Alice
Server

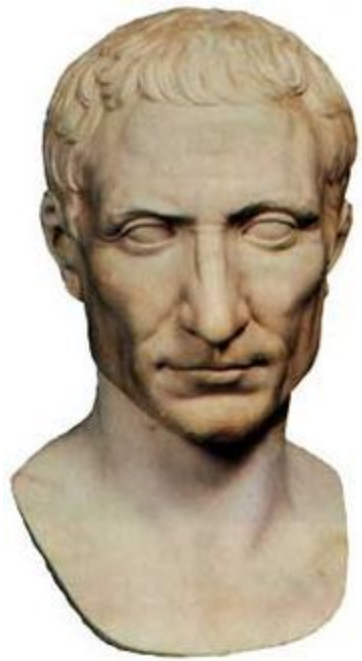
math.unl.edu - PuTTY

```
math> telnet www.math.unl.edu 80
Trying 129.93.180.31...
Connected to www.math.unl.edu.
Escape character is '^]'.
POST /~jorr1/presentations/2007/ea/toaster/form.php HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 62

name=Harry Potter&card=7890 5678 9877 1111&type=Gringotts Bank
HTTP/1.1 200 OK
Date: Mon, 26 Feb 2007 13:39:36 GMT
Server: Apache/2.0.52 (CentOS)
X-Powered-By: PHP/4.3.9
Content-Length: 379
Connection: close
Content-Type: text/html

<html>
  <head>
    <title>Order Confirmation</title>

    <style>
      @import URL("style.css");
    </style>
  </head>

  <body>

    <h1>Order Confirmation</h1>

    Hi Harry Potter.<br>
    Your card number is 7890 5678 9877 1111.<br>
    It's a Gringotts Bank card.
    <p>
    Your USB Toaster will be winging it's way to you soon...
  </body>
</html>
Connection closed by foreign host.
math>
```

Codes and Ciphers

Julius Caesar and MI5

…if he had anything confidential to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet, that not a word could be made out. If anyone wishes to decipher these, and get at their meaning, he must substitute the fourth letter of the alphabet, namely D, for A, and so with the others.



…si qua occultius perferenda erant, per notas scripsit, id est sic structo litterarum ordine, ut nullum uerbum effici posset: quae si qui inuestigare et persequi uelit, quartam elementorum litteram, id est D pro A et perinde reliquas commutet.

Suetonius
Life of Julius Caesar, 56

math.unl.edu - PuTTY

```
math> telnet www.math.unl.edu 80
Trying 129.93.180.31...
Connected to www.math.unl.edu.
Escape character is '^]'.
POST /~jorr1/presentations/2007/ea/toaster/form.php HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 62

name=Harry Potter&card=7890 5678 9877 1111&type=Gringotts Bank
HTTP/1.1 200 OK
Date: Mon, 26 Feb 2007 13:39:36 GMT
Server: Apache/2.0.52 (CentOS)
X-Powered-By: PHP/4.3.9
Content-Length: 379
Connection: close
Content-Type: text/html

<html>
  <head>
    <title>Order Confirmation</title>

    <style>
      @import URL("style.css");
    </style>
  </head>

  <body>

    <h1>Order Confirmation</h1>

    Hi Harry Potter.<br>
    Your card number is 7890 5678 9877 1111.<br>
    It's a Gringotts Bank card.
    <p>
    Your USB Toaster will be winging it's way to you soon...
  </body>
</html>
Connection closed by foreign host.
math>
```

"… substitute the fourth letter of the alphabet, namely D, for A, and so with the others…"

H a r r y P o t t e r

~~K~~H d u u ~~b~~y S r w w h u

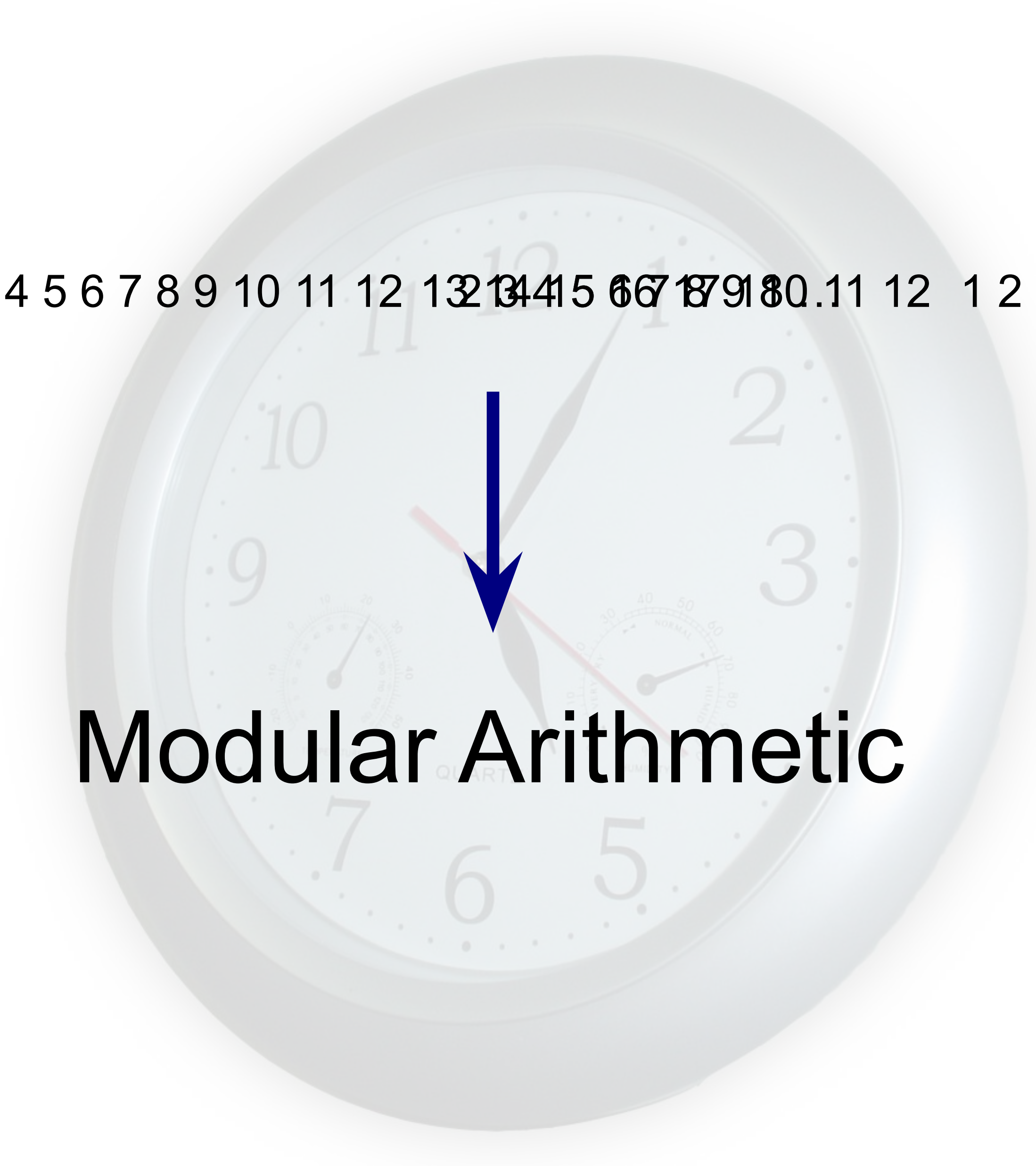
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2

A H R Y

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2

D K U B

K D U U B



1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 …

1 2 3 4 5 6 7 8 9 10 11 12 1 2 3 4 5 6 …

Modular Arithmetic

$$a \equiv b \pmod{m}$$

$a - b$ is a multiple of m

$$10 + 3 \equiv 1 \pmod{12}$$

$$(10+3) - 1 = 13 - 1 = 12 = 1 \times 12$$

$$2 - 6 \equiv 8 \pmod{12}$$

$$(2-6) - 8 = -4 - 8 = -12 = -1 \times 12$$

H

$$7 + 3 \equiv 10 \pmod{26}$$

K

A

$$0 + 3 \equiv 3 \pmod{26}$$

D

R

(twice)

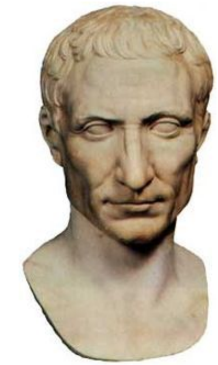
$$17 + 3 \equiv 20 \pmod{26}$$

U

Y

$$24 + 3 \equiv 1 \pmod{26}$$

B



Caesar Cipher

H

$$7 + \boxed{3} \equiv 10 \pmod{26}$$

K

A

$$0 + \boxed{6} \equiv 6 \pmod{26}$$

G

R
(twice)

$$17 + \boxed{9} \equiv 0 \pmod{26}$$

A

Y

$$24 + \boxed{12} \equiv 10 \pmod{26}$$

K

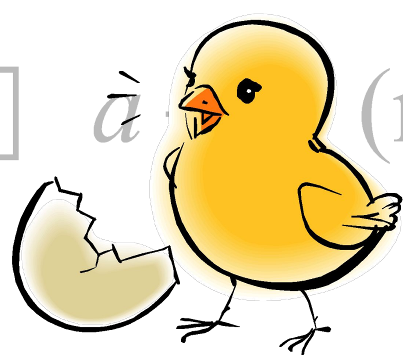
Polyalphabetic Cipher

A **cipher** is a set of rules for encrypting data.

$$E : a \mapsto a + 3 \pmod{26}$$

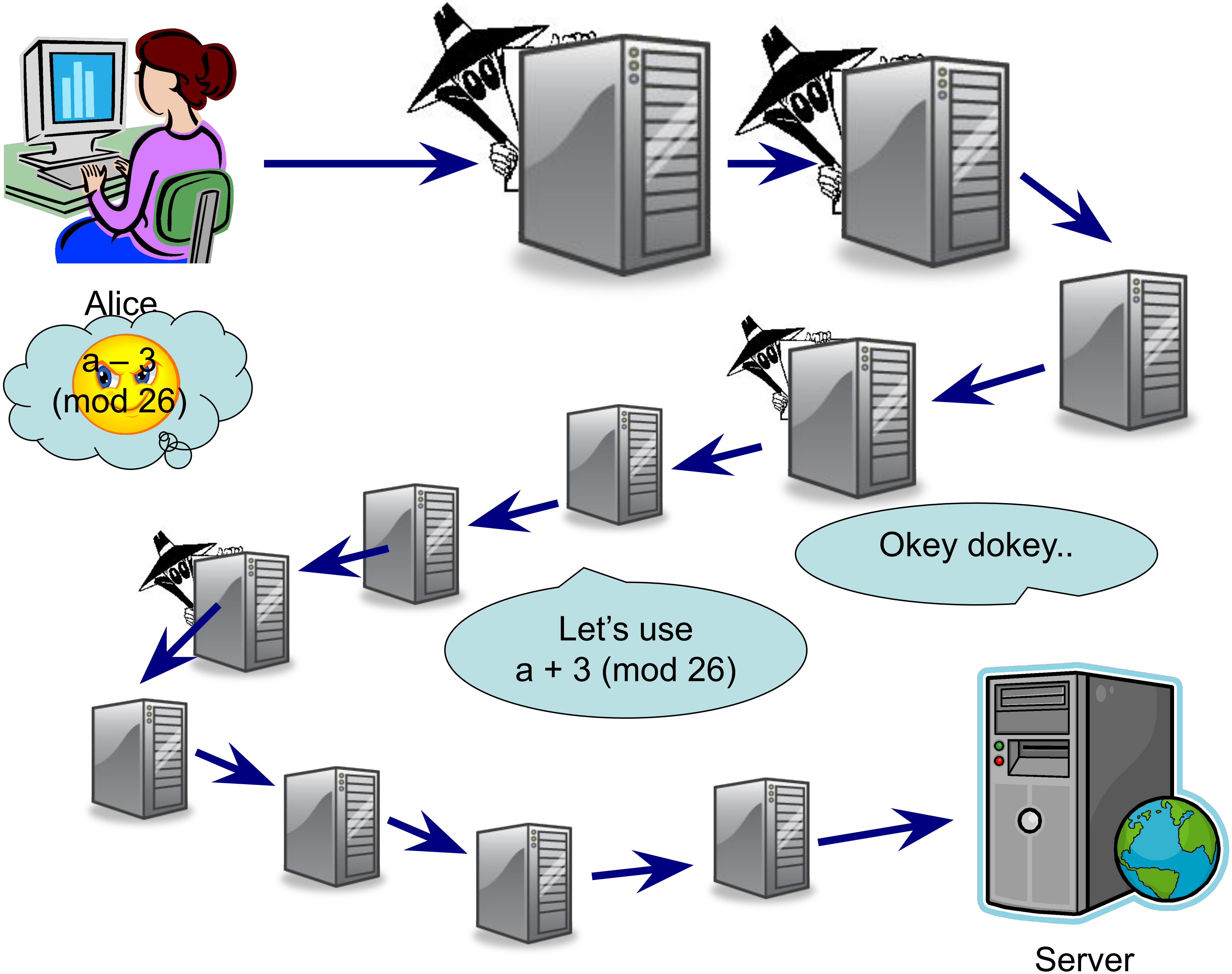
A cipher is **symmetric** if knowledge of the information needed to encrypt also gives you knowledge of how to decrypt.

$$D : a \mapsto a \quad \ldots \quad (\mathrm{mod}\ 26)$$



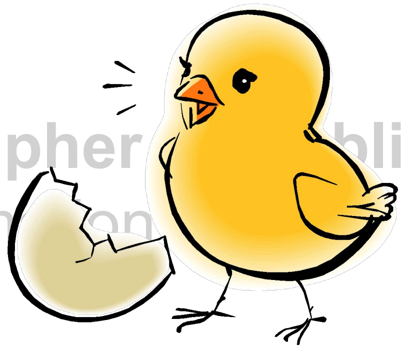
The Chicken and the Egg

Symmetric and asymmetric ciphers



Alice
a – 3 (mod 26)
Okey dokey..
Let's use
a + 3 (mod 26)
Server

An **asymmetric cipher** **blic key cipher**, is one where knowing the inform on to encrypt doesn't help you decrypt.

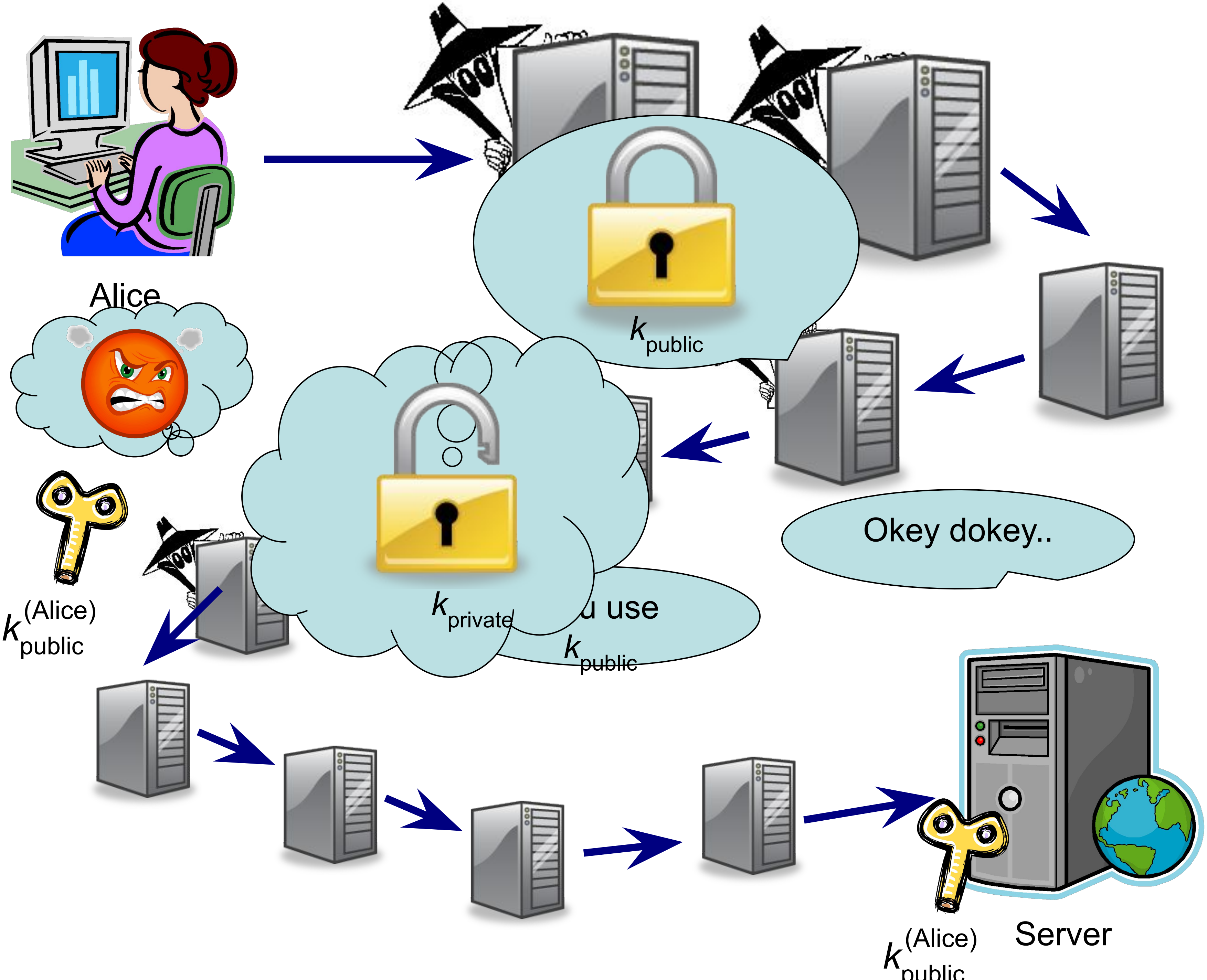


An asymmetric cipher has two parts:

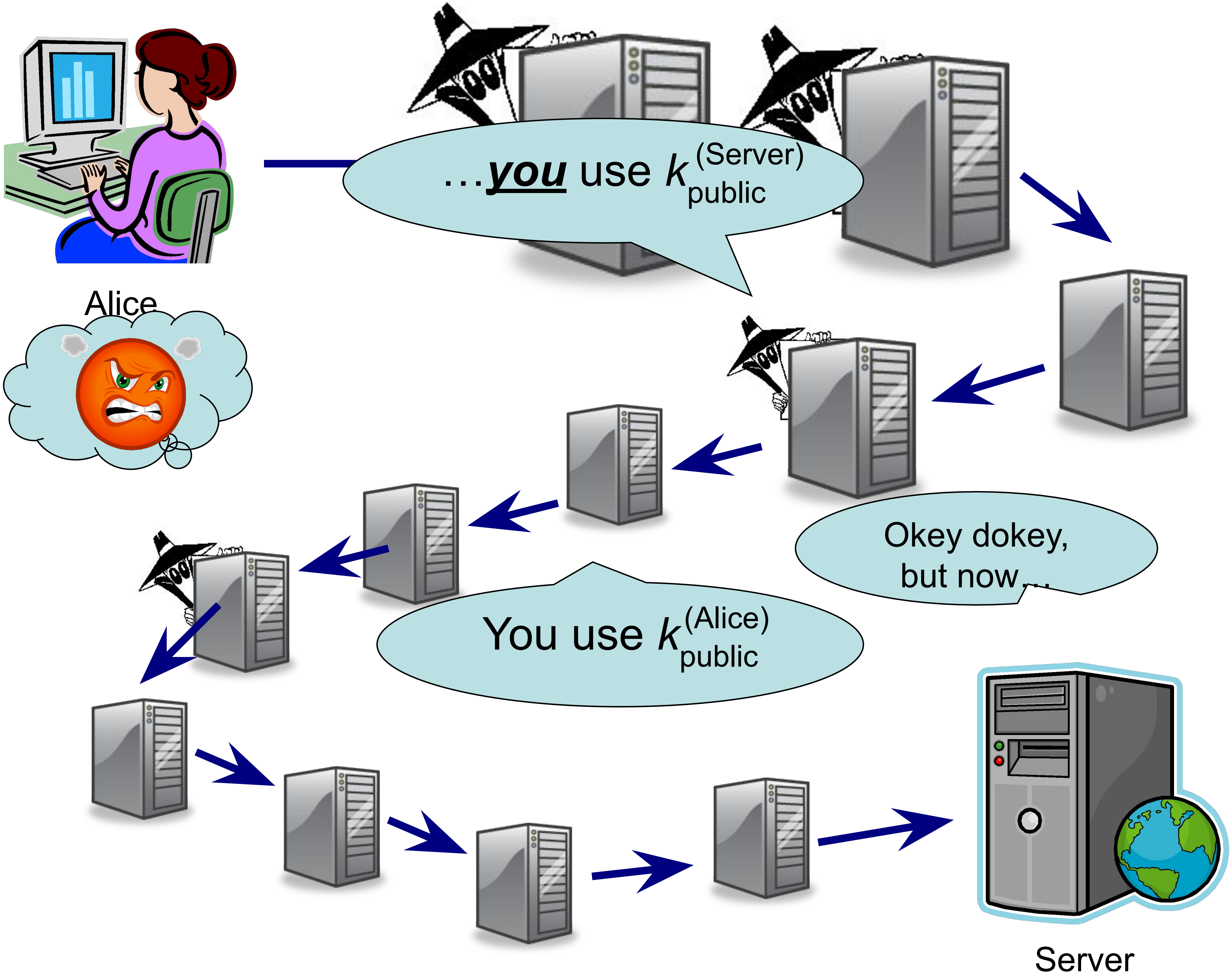
A **public key** k_{public} encrypts

A **private key** k_{private} decrypts

Keep the private key secret – give the public key to anyone.



Alice
k_{public}
$k_{private}$
Okey dokey..
u use
k_{public}
$k^{(Alice)}_{public}$
$k^{(Alice)}_{public}$
Server



…*you* use $k^{(Server)}_{public}$
Alice
Okey dokey, but now…
You use $k^{(Alice)}_{public}$
Server

525,600 Minutes

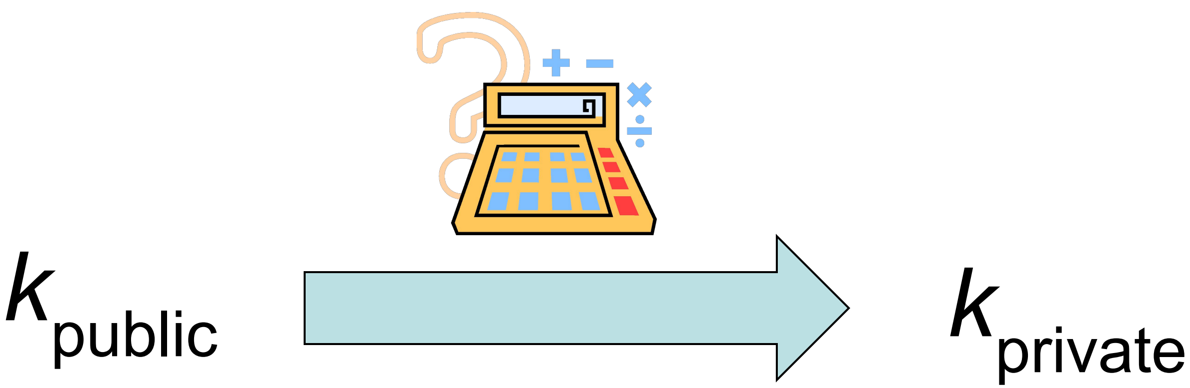
Why asymmetric ciphers work

So:

An **asymmetric cipher**, or **public key cipher**, is one where knowing the information needed to encrypt doesn't help you decrypt.

How is this possible?

In fact, k_{public} and $k_{private}$ *are* related, but…



RSA Public Key Cryptography

Described by

Rob Rivest, Adi Shamir, and Leonard Adleman

at MIT in 1977.

The idea is based on **prime numbers**…

A **prime number** is one whose only factors are 1 and itself.

e.g. 2, 3, 5, 7, 11, 13 but not 4, or 6

Theorem. *Every number is the product of prime numbers.*

e.g. 1,386 = 2×693 = 2×3×231 = 2×3×3×77=2×3×3×7×11

Theorem. *There is no biggest prime number.*

If 2,3,5,7,…,P were all the prime numbers then what about

$$1 + 2 \times 3 \times 5 \times 7 \times \ldots \times P$$

Each of these numbers is the product of *exactly* **two** prime numbers. What are they?

$$6 = 2 \times 3$$

$$10 = 2 \times 5$$

$$21 = 3 \times 7$$

$$221 = 13 \times 17$$

$$713 = 23 \times 31$$

$$456{,}989{,}977{,}669 = 611{,}953 \times 746{,}773$$

$$= P_{5000} \times P_{6000}$$

The RSA **public** key consists of a number which is the product of two prime numbers. If you could figure out *which* two prime numbers you could find the **private** key.

“Ask a computer – computers are good at these kind of things…”

Look again at

$$456{,}989{,}977{,}669 = 611{,}953 \times 746{,}773$$

One way to factor 456,989,977,669 is to check all the numbers 1,2,3,… up to $\sqrt{456{,}989{,}977{,}669} \approx 676{,}010$.

If a computer can do 1,000,000 tests in a second, then it can do this in just 676,010 ÷ 1,000,000 = 0.676 seconds.

But what if N = P×Q is 100 digits long?

Then

$$10^{99} \le N < 10^{100}$$

so

$$10^{49} \le \sqrt{N} < 10^{50}$$

and the computer can solve it in

$$10^{50} \div 10^{6} = 10^{44} \text{ seconds.}$$

10^{44} = 100,000,000,000,000,000,000,000,000,000,000,000,000,000,000 seconds

There are

$$60 \times 24 \times 365 = 525{,}600 \text{ minutes in a year}$$

and so there are

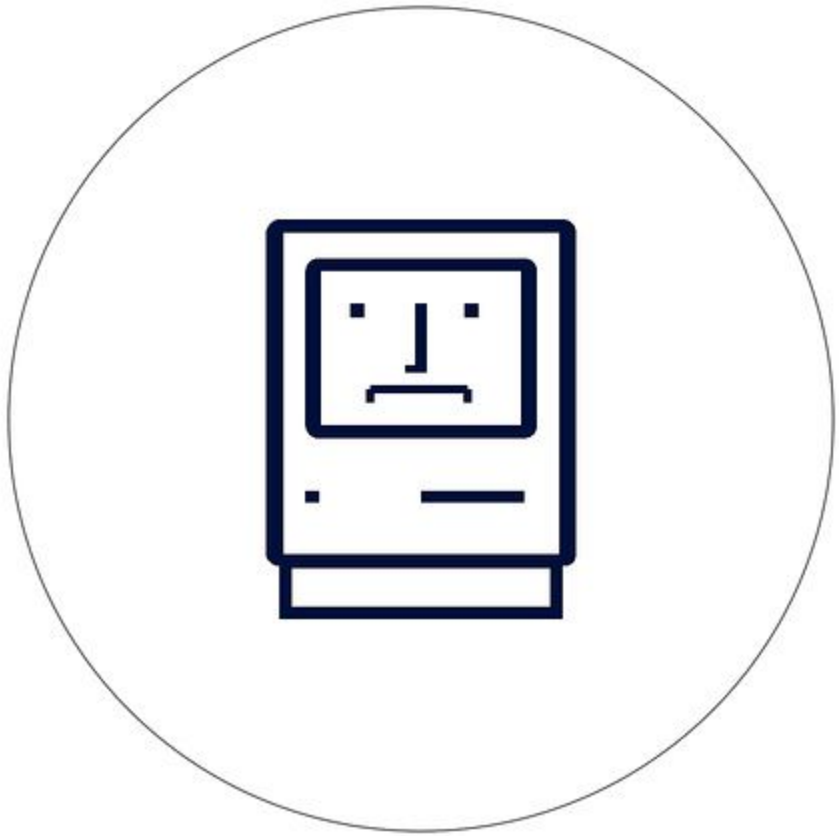
$$60 \times 525{,}600 = 31{,}536{,}000 \text{ seconds.}$$

So 10^{44} seconds is

$$\frac{10^{44}}{31{,}536{,}000} \approx 3.17 \times 10^{36} \text{ years}$$

That's 3,170,000,000,000,000,000,000,000,000,000,000,000 years

Age of the universe = 13,700,000,000 years



Theorem. *There is no biggest prime number.*

And we have good algorithms for finding very big prime numbers (100's of digits)

But we have no methods of finding the prime factors of $N=PQ$ that are *qualitatively* better than just checking all possibilities:

$$T = C\,A^d \quad \text{where } d = \#\text{ digits in } N$$

How does RSA work?

Need to generate a **public** and a **private** key.

Step 1: Pick two (very) big prime numbers p and q

Step 2: Pick a number $0 < r < (p-1)(q-1)$

Step 3: Find a number $0 < s < (p-1)(q-1)$ such that

$$rs \equiv 1 \pmod{(p-1)(q-1)}$$

Key Fact: For any number x,

$$a \equiv b \pmod{m}$$

$$x^{rs} \equiv x \pmod{pq}$$

$$a - b \text{ is a multiple of } m$$

$$rs - 1 \text{ is a multiple of } (p-1)(q-1)$$

How does RSA work? (cont…)

Key Fact: For any number *x*,

$$x^{rs} \equiv x \pmod{pq}$$

Let $n = pq$

Why does it work?

Public Key: n and

Private Key: n and s

$$y \equiv x^r \pmod{pq}$$

$$\Rightarrow y^s \equiv x^{rs} \equiv x \pmod{pq}$$

Now, given x…

To **encode** x: Calculate y = the remainder of $x^r \div n$

To **decode** y: Calculate the remainder of $y^s \div n$

$$\boxed{x^{rs} \equiv x \pmod{pq}}$$

$$rs \equiv 1 \pmod{(p-1)(q-1)}$$

$$rs - 1 = k(p-1)(q-1)$$

$$rs = 1 + k(p-1)(q-1)$$

$$\begin{aligned} x^{rs} = x^{1+k(p-1)(q-1)} &= x \cdot \left(x^{(p-1)(q-1)}\right)^k \\ &\equiv x \cdot (1)^k \equiv x \pmod{pq} \end{aligned}$$

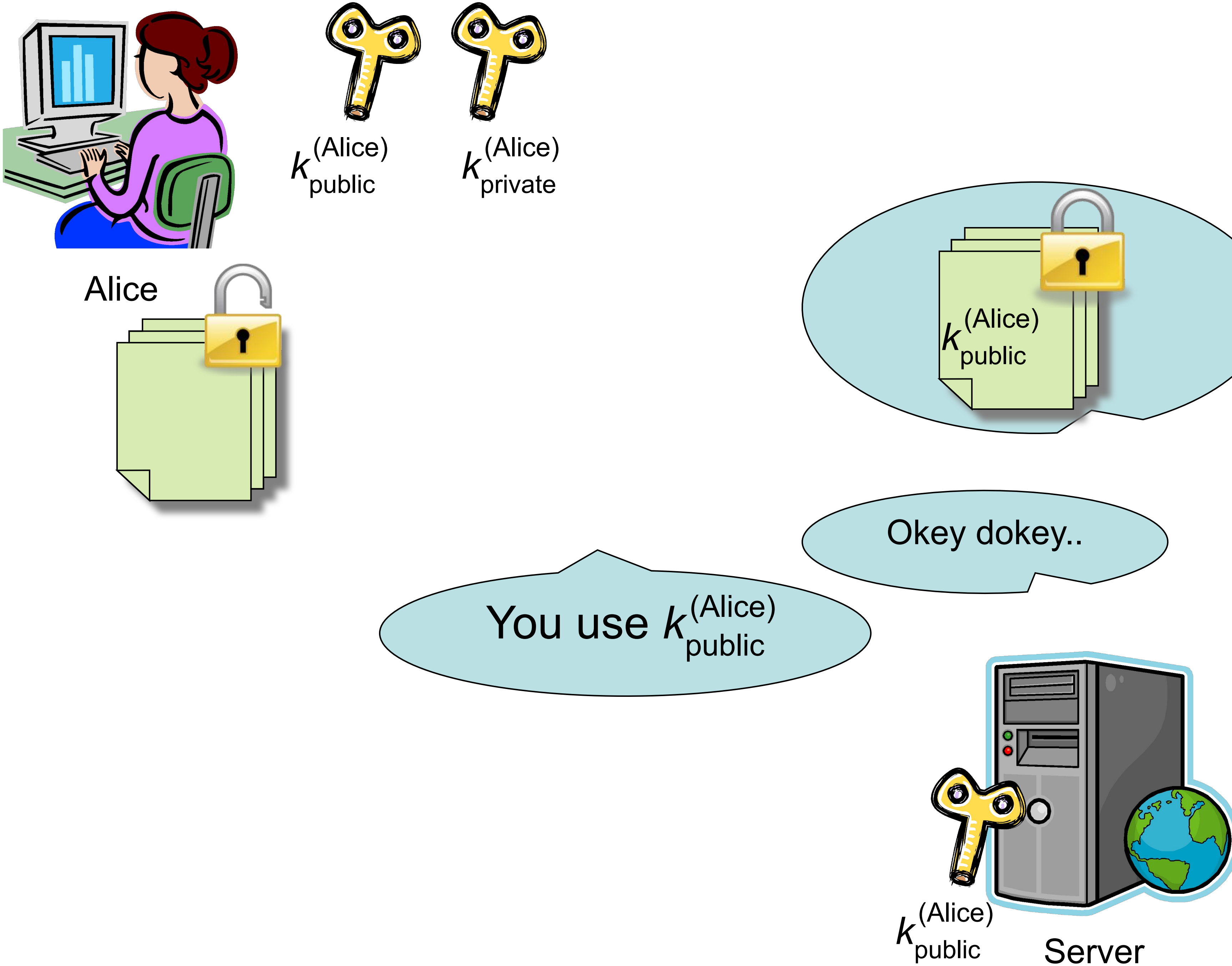
$$x^{p-1} \equiv 1 \pmod{p}$$ "Fermat's Little Theorem"

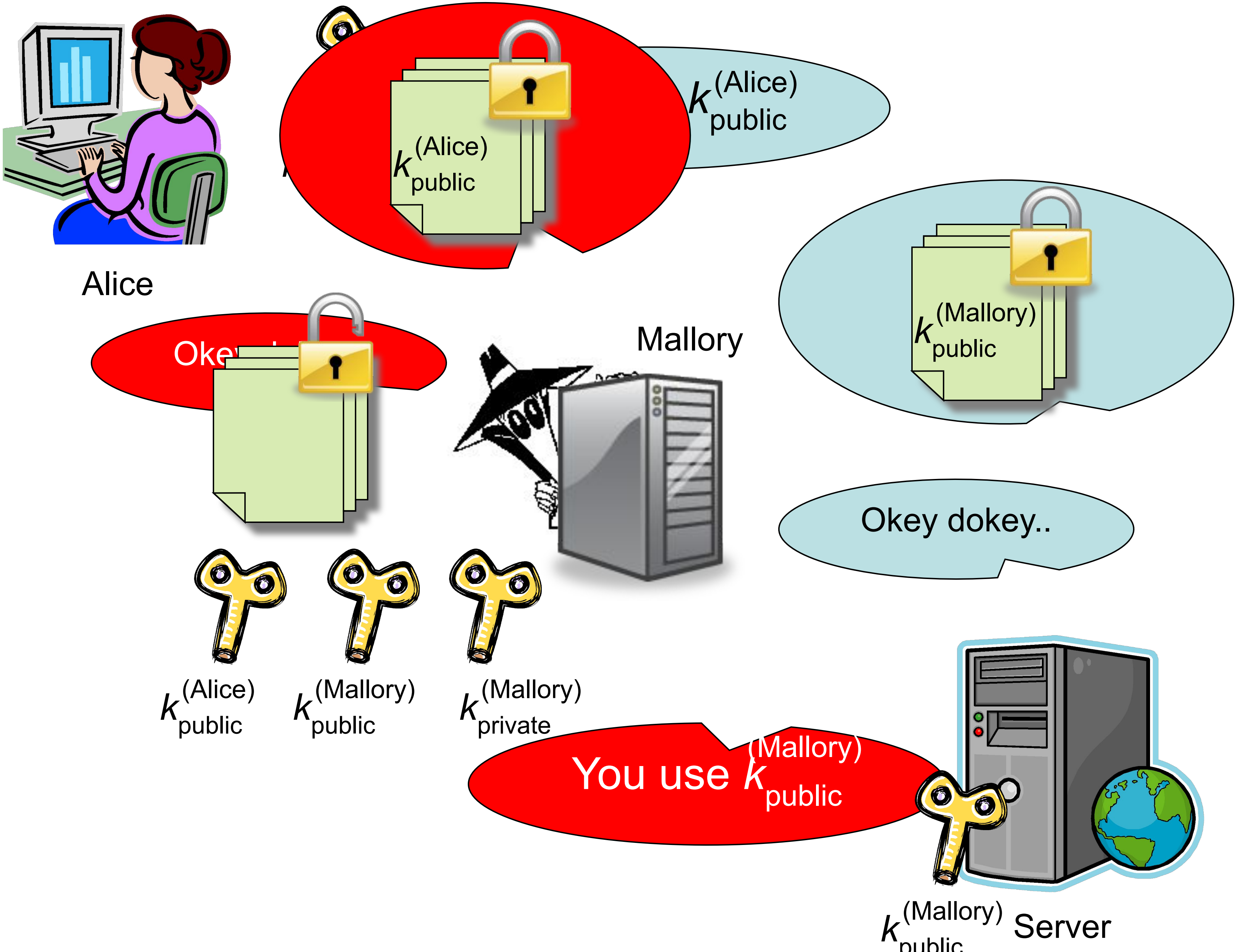
$$x^{q-1} \equiv 1 \pmod{q}$$

$$x^{(p-1)(q-1)} \equiv 1 \pmod{pq}$$ "Chinese Remainder Theorem"

The Bad Guys Get Smart

Man-in-the-middle attacks


$k^{(Alice)}_{public}$
$k^{(Alice)}_{private}$
Alice
$k^{(Alice)}_{public}$
Okey dokey..
You use $k^{(Alice)}_{public}$
$k^{(Alice)}_{public}$
Server

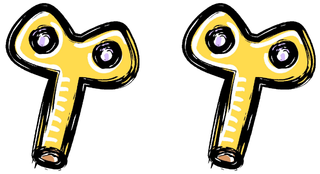


Alice
$k^{(Alice)}_{public}$
$k^{(Alice)}_{public}$
Mallory
$k^{(Mallory)}_{public}$
Okey dokey..
$k^{(Alice)}_{public}$
$k^{(Mallory)}_{public}$
$k^{(Mallory)}_{private}$
You use $k^{(Mallory)}_{public}$
$k^{(Mallory)}_{public}$
Server

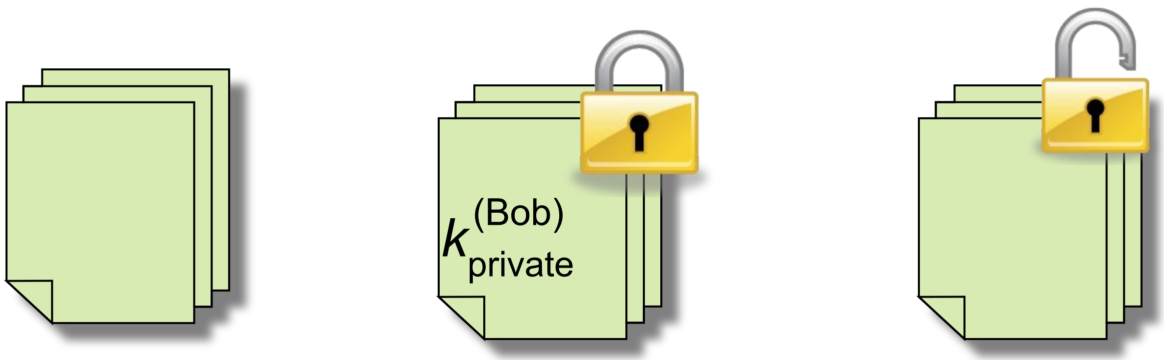
Digital Signatures

Digital Signatures

Bob



$k^{(Bob)}_{public}$ $k^{(Bob)}_{private}$

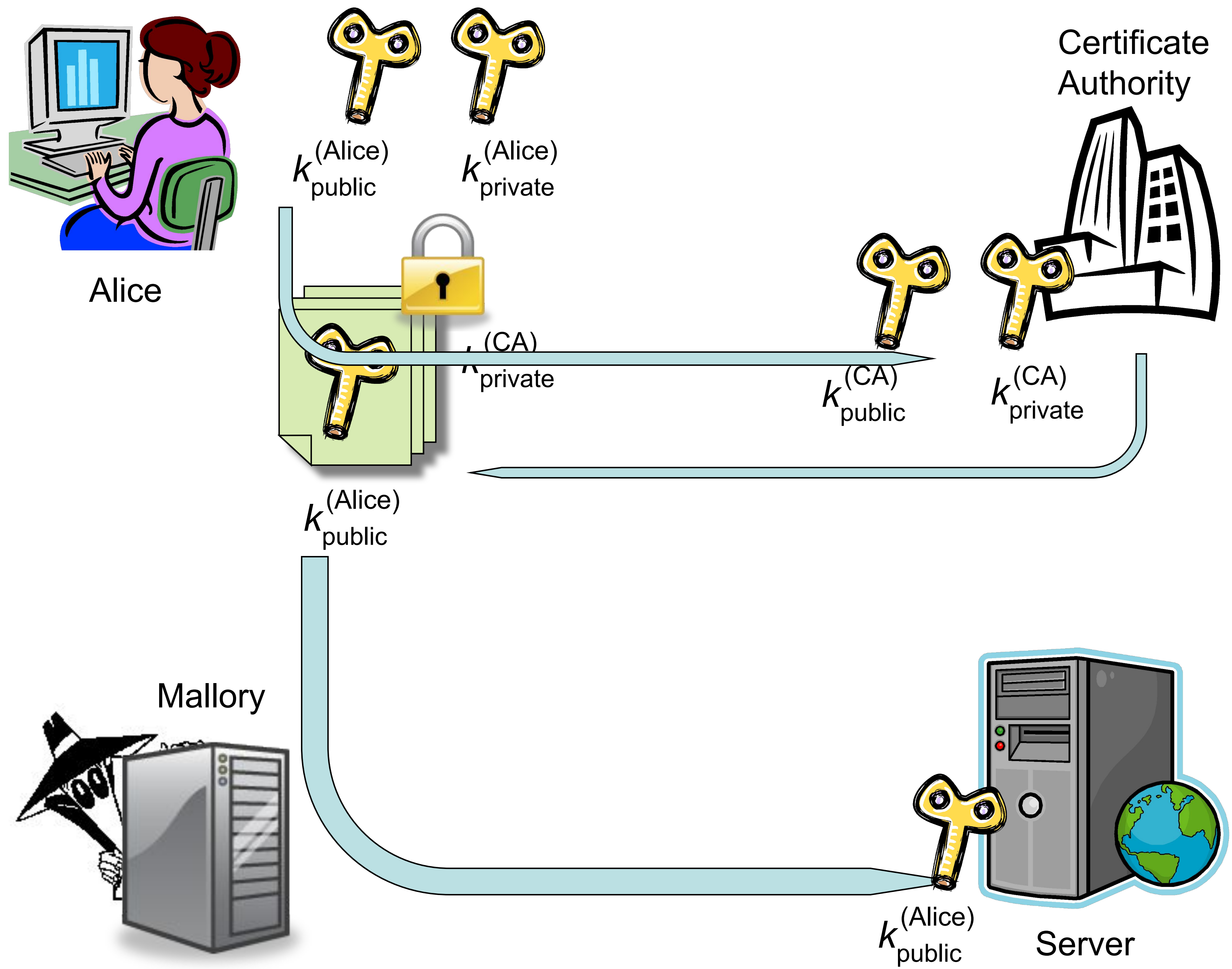


Anyone can read the message…

…but only **one** person could have <u>*written*</u> the message…

Bob!

$k^{(Bob)}_{public}$

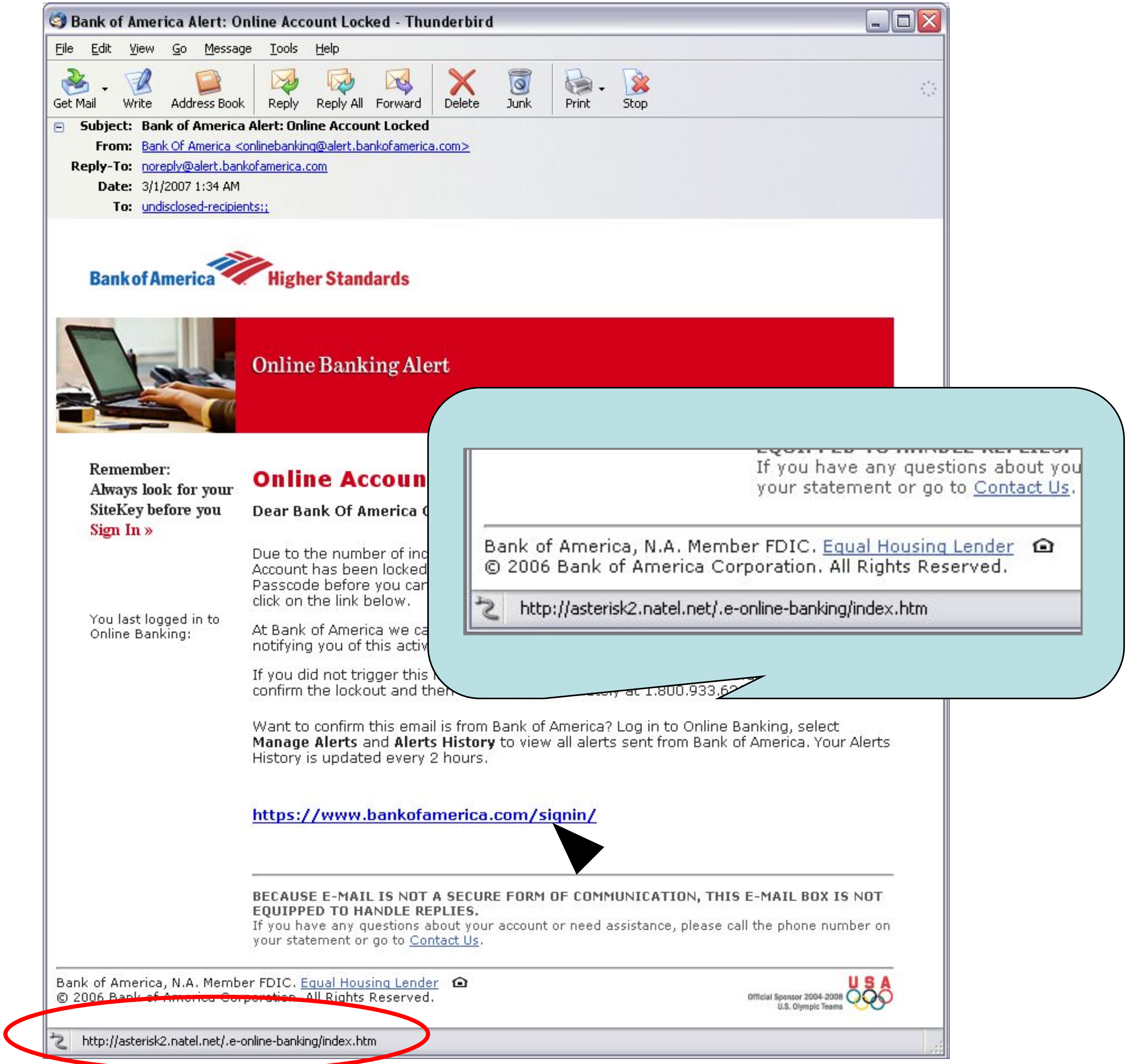


Alice
$k^{(Alice)}_{public}$
$k^{(Alice)}_{private}$
Certificate Authority
$k^{(CA)}_{private}$
$k^{(CA)}_{public}$
$k^{(CA)}_{private}$
$k^{(Alice)}_{public}$
Mallory
$k^{(Alice)}_{public}$
Server

Security Ain’t Safety

Phishing


Order your USB toaster here! - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://www.math.unl.edu/~jorr1/presentations/2007/ea/toaster/
The Amazing USB Toaster
Name: Harry Potter
Credit Card Number: 7890 5678 9877 1111
Credit Card Type: Gringotts Bank
Buy It Now!
Fresh on-the-go toast!
• Lightweight! Only 2.3 pounds
• Make up to four pieces of toast in 30 minutes!
• Runs off any laptop's USB port*
DigiPliance
USB Toaster
Single Slice USB Powered Toasting Computer Accessory
BIG OL' FLAP ON EACH END
GOTCHA!
SALT OF THE MONTH CLUB
MAKE-YOUR-OWN Umbrella Kit
Done
www.math.unl.edu


Bank of America Alert: Online Account Locked - Thunderbird
File Edit View Go Message Tools Help
Get Mail Write Address Book Reply Reply All Forward Delete Junk Print Stop
Subject: Bank of America Alert: Online Account Locked
From: Bank Of America <onlinebanking@alert.bankofamerica.com>
Reply-To: noreply@alert.bankofamerica.com
Date: 3/1/2007 1:34 AM
To: undisclosed-recipients:;
Bank of America Higher Standards
Online Banking Alert
Remember:
Always look for your SiteKey before you
Sign In »
You last logged in to Online Banking:
Online Accoun
Dear Bank Of America C
Due to the number of inc
Account has been locked
Passcode before you can
click on the link below.
At Bank of America we ca
notifying you of this activ
If you did not trigger this
confirm the lockout and then
Want to confirm this email is from Bank of America? Log in to Online Banking, select Manage Alerts and Alerts History to view all alerts sent from Bank of America. Your Alerts History is updated every 2 hours.
https://www.bankofamerica.com/signin/
BECAUSE E-MAIL IS NOT A SECURE FORM OF COMMUNICATION, THIS E-MAIL BOX IS NOT EQUIPPED TO HANDLE REPLIES.
If you have any questions about your account or need assistance, please call the phone number on your statement or go to Contact Us.
Bank of America, N.A. Member FDIC. Equal Housing Lender
© 2006 Bank of America Corporation. All Rights Reserved.
Official Sponsor 2004-2008 U.S. Olympic Teams
http://asterisk2.natel.net/.e-online-banking/index.htm
If you have any questions about you
your statement or go to Contact Us.
Bank of America, N.A. Member FDIC. Equal Housing Lender
© 2006 Bank of America Corporation. All Rights Reserved.
http://asterisk2.natel.net/.e-online-banking/index.htm

http://www.math.unl.edu/~jorr/presentations