CRYPTOGRAPHY

1. Really Big Numbers

One of the things I've used on the Google is to pull up maps…

You've probably used the Google, too!

Do you know where this company's strange name comes from?

Extract from *Mathematics and the Imagination,* by Edward Kasner and James R. Newman, 1940.

Words of wisdom are spoken by children at least as often as by scientists. The name "googol" was invented by a child (Dr. Kasner's nine-year-old nephew) who was asked to think up a name for a very big number, namely 1 with a hundred zeros after it….At the same time he suggested "googol" he gave a name for a still larger number: "Googolplex." …It was first suggested that a googolplex should be 1, followed by writing zeros until you got tired. This is a description of what would happen if one actually tried to write a googolplex, but different people get tired at different times…The googolplex, then, is a specific finite number, with so many zeros after the 1 that the number of zeros is a googol.

Moral

- You can write a googol (it will only take a minute).
- But you can’t write a googolplex---that is, you can’t write down a googol zeros, or count up to a googol.
- Even a computer would get tired long before it succeeded in doing this.

googol = 10^{100}

googolplex = $10^{\text{googol}} = 10^{10^{100}}$

- If one trillion computers carried out one trillion operations a second, for one trillion years, they would perform fewer than 10^{44} operations.

googol = 10^{100}

googolplex = $10^{\text{googol}} = 10^{10^{100}}$

- If one trillion computers performed one trillion operations a second, for one trillion years, they would perform fewer than 10^{44} operations.
- If you repeat this experiment on a trillion trillion different planets, you will perform about 10^{92} operations in all.

2. Let’s Buy Something to

Amazon.com: Mathematics and the Imagination: Edward Kasner,James Newman: Books

http://www.amazon.com/Mathematics-Imagination-Edward-Kasner/dp/0486417034/ref=pd_bbs_s

Getting Started | Latest Headlines | Apple | Amazon | eBay | Yahoo! | News

2005 Fall Central Section ... | ScienceDirect - Journal of ... | Journal of Algebra - Elsevier | Scrabulous | Your Email Ga... | Amazon.com: Mathematics...

amazon.com

Hello, H Straubing. We have recommendations for you. (Not H?)

H's Amazon.com | Today's Deals | Gifts & Wish Lists | Gift Cards | Your Account | Help

Shop All Departments | Search Books | GO | Cart | Your Lists

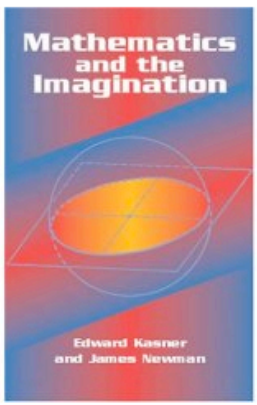
Books | Advanced Search | Browse Subjects | Hot New Releases | Bestsellers | The New York Times® Best Sellers | Libros En Español | Bargain Books | Textbooks

Prime

To get this item by **Friday**, April 25 order within 4hr 36min.

Get Free Shipping for a full month with a Free Trial of Amazon Prime › learn more

FREE Upgrade to Two-Day Shipping on this item with Amazon Prime



See larger image

Share your own customer images

Publisher: learn how customers can search inside this book.

Are You an Author or Publisher? Find out how to publish your own Kindle Books

Mathematics and the Imagination (Paperback)

by Edward Kasner (Author), James Newman (Author)

(8 customer reviews)

List Price: ~~$15.95~~

Price: $10.85 & eligible for **FREE Super Saver Shipping** on orders over $25. Details

You Save: $5.10 (32%)

In Stock.

Ships from and sold by **Amazon.com**. Gift-wrap available.

Want it delivered Thursday, April 24? Order it in the next 4 hours and 36 minutes, and choose **One-Day Shipping** at checkout. See details

16 used & new available from $9.82

Also Available in:	List Price:	Our Price:	Other Offers:
Hardcover			4 used & new from $7.85
Paperback (New Ed)			10 used & new from $2.85
Unknown Binding			9 used & new from $4.24

Quantity: 1

Add to Shopping Cart

or

Sign in to turn on 1-Click ordering.

More Buying Choices

16 used & new from $9.82

Have one to sell? Sell yours here

Add to Wish List

Add to Shopping List

Add to Wedding Registry

Add to Baby Registry

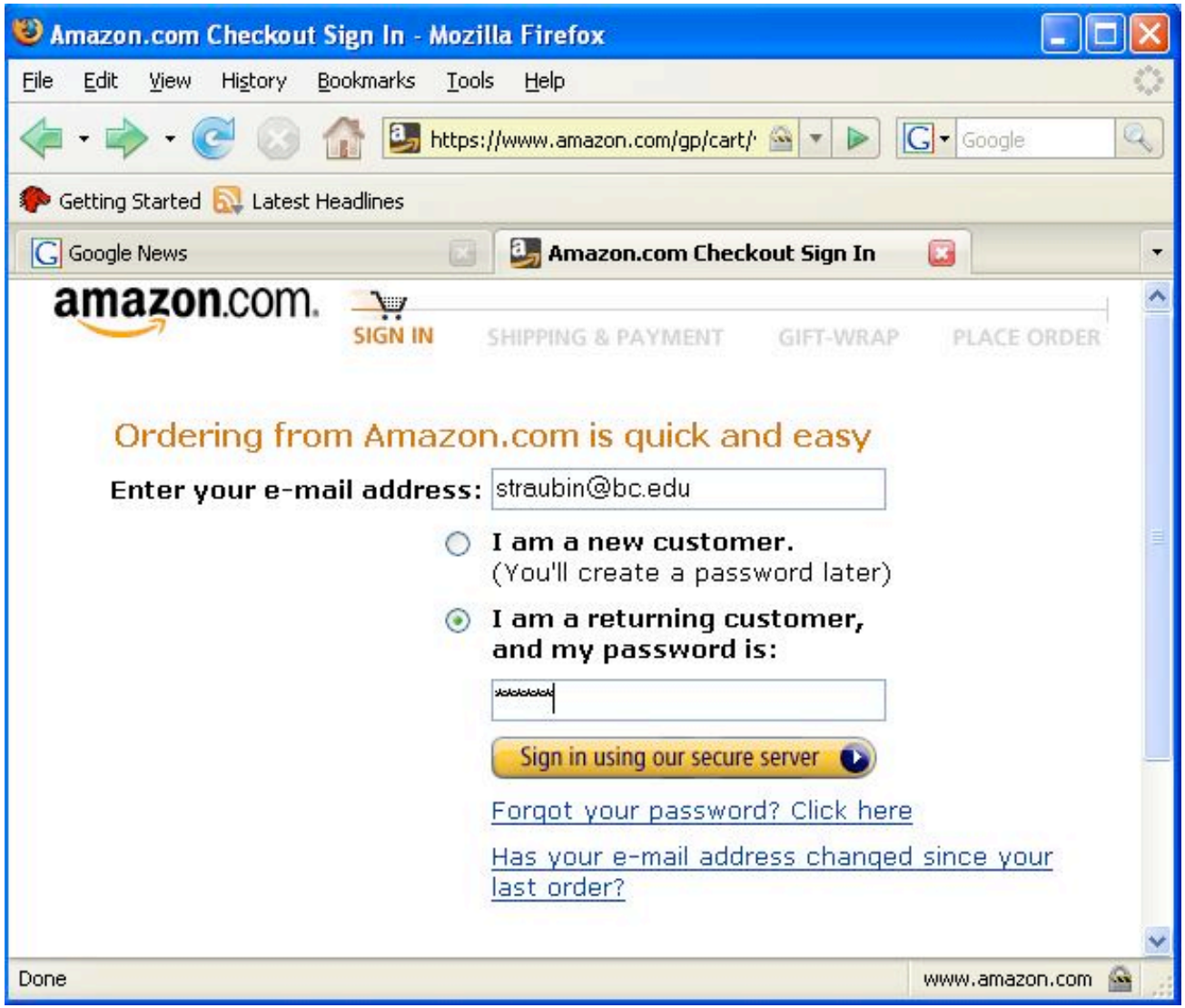
Tell a friend

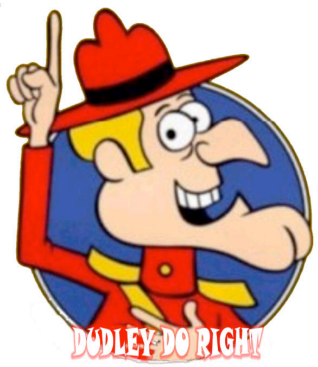
Better Together

Buy this book with One Two Three . . . Infinity: Facts and Speculations of Science by George Gamow today!

Done

Is That Safe?


Amazon.com Checkout Sign In - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://www.amazon.com/gp/cart/
Google
Getting Started
Latest Headlines
Google News
Amazon.com Checkout Sign In
amazon.com.
SIGN IN
SHIPPING & PAYMENT
GIFT-WRAP
PLACE ORDER
Ordering from Amazon.com is quick and easy
Enter your e-mail address:
straubin@bc.edu
I am a new customer.
(You'll create a password later)
I am a returning customer,
and my password is:
Sign in using our secure server
Forgot your password? Click here
Has your e-mail address changed since your last order?
Done
www.amazon.com



BOB

My password is "Nell"

You're in!

My credit card number is 123456789

ALICE
(an Amazon?)

Someone Might be Listening!

BOB

My password is "Nell"

You're in!

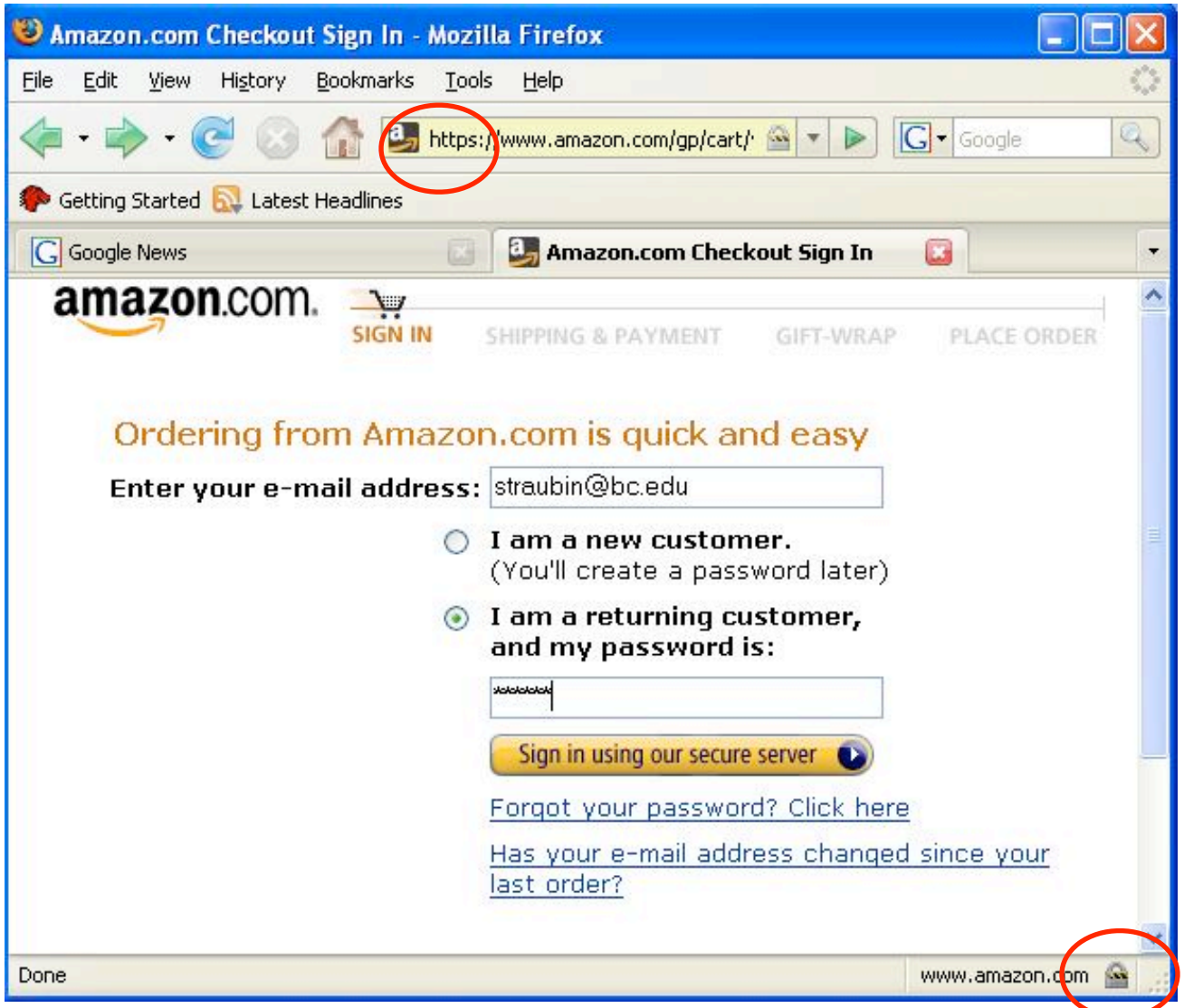
My credit card number is 123456789

SNIDELY

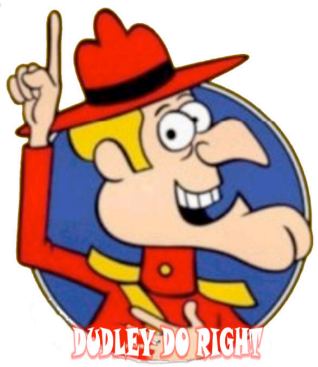
Nyeh-heh-heh

ALICE

Sensitive Information Sent over the Internet is *Encrypted* by the Sender's Computer, and *Decrypted* by the Recipient



Someone is still listening, but learns nothing



BOB

*Skdn9(&*osaj.v,420kja* →

← *$%^*J<}++UUY*

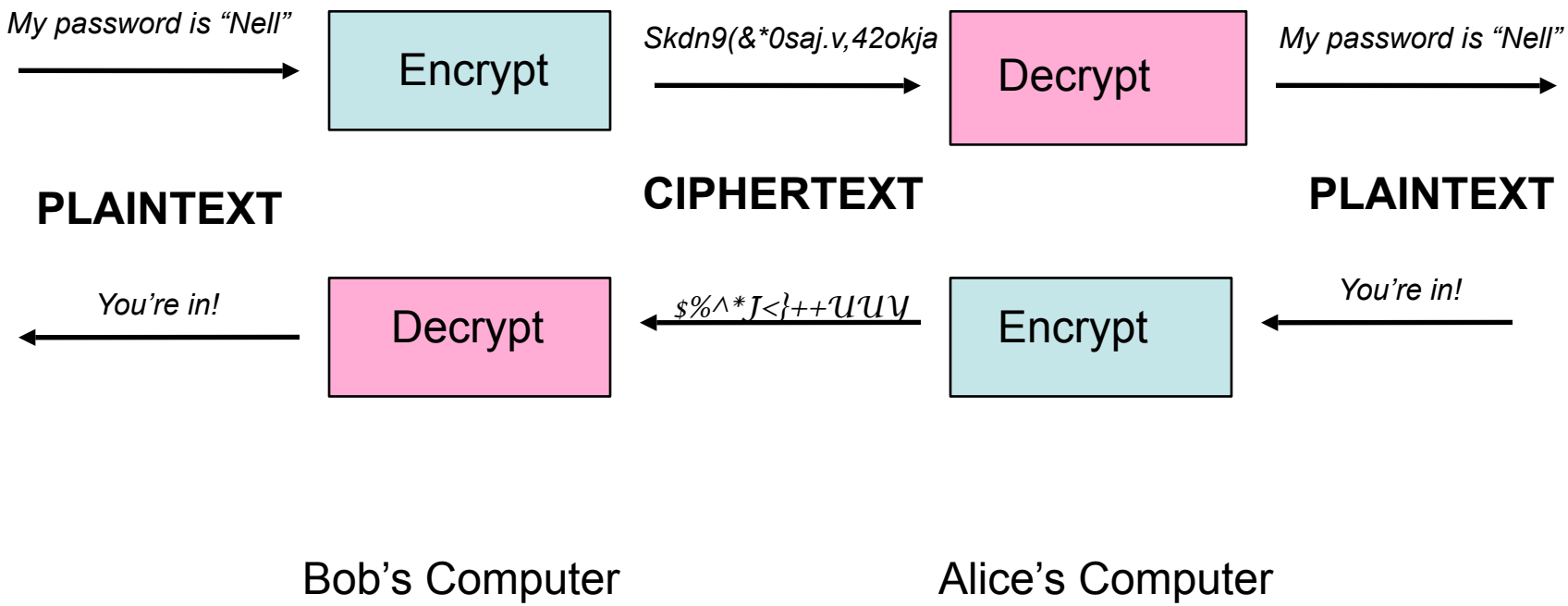
BG&98JIJ I7656><J^%+{'}* →

ALICE

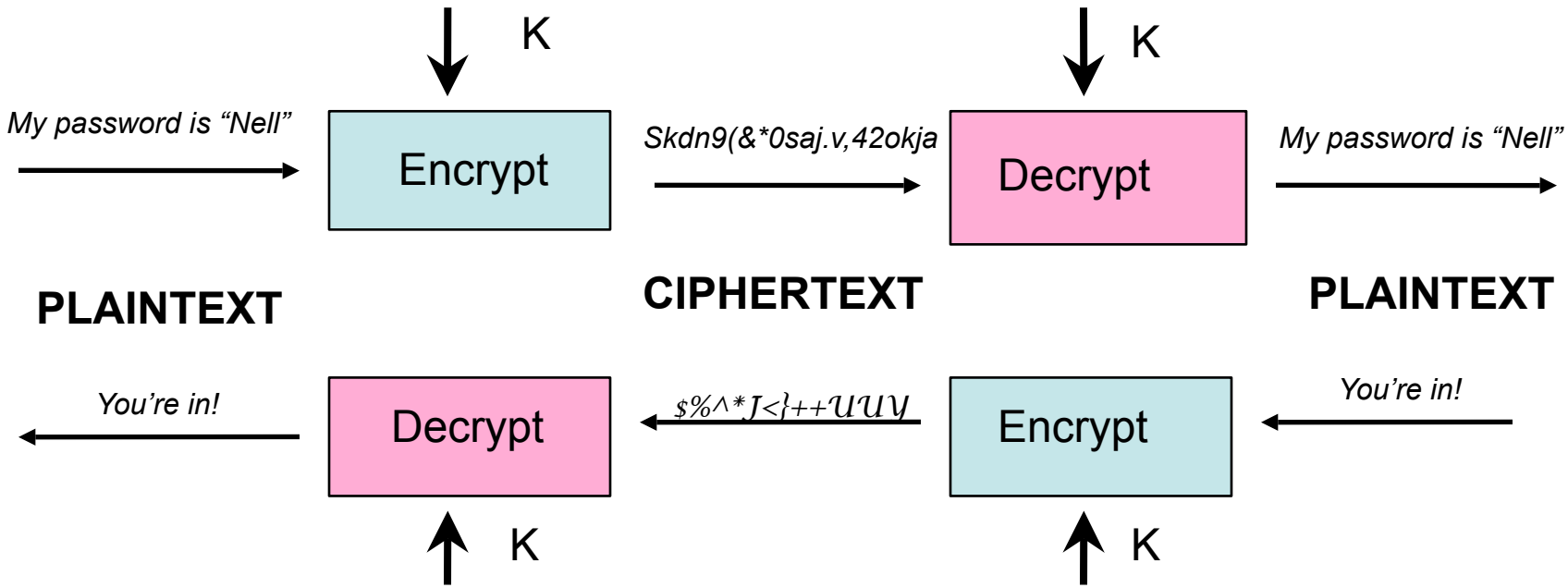
SNIDELY

Curses! Foiled again!

Both parties run programs to carry out the encryption and decryption



The programs are publicly available (they're built into your Web browser). So Alice and Bob must share some additional, *secret*, information—a "key"



It should be for all practical purposes impossible for an eavesdropper to guess the key K.

The Central Metaphor of Cryptography

You need the key both to lock and unlock the treasure chest. Alice and Bob are the only people with keys.

Example of a (bad) cryptographic system-Cryptogram Puzzles

Ugsxqxai xi qez wzyqsz pvq gj wzqqxyw fgqzi jvgl qez uggv pyh aplupxwy jdyhi jvgl qez vxae om uvglxixyw qg uvgqzaq zpae jvgl qez gqezv.

Each letter of the alphabet is replaced by a different letter.
The Key tells which letter replaces A, which replaces B, etc., and the encryption and decryption algorithms apply this replacement procedure—and its inverse--- to each letter of the plaintext or ciphertext.

Example-Cryptogram Puzzles

Ugsxqxaixiqezwzyqszpvqgjwzqqxywfgqez
uggvpyhaplupxwyjdyhijvglqezvxaeomuvglx
ixywqguvgqzaqzpaejvglqezgqezv.

This makes the puzzle more interesting!

A *Huge* Number of Possible Keys

- For such puzzles the key is a permutation (rearrangement) of "ABCDEFGHIJKLMNOPQRSTUVWXYZ".

- There are

$26! = 26 \times 25 \times 24 \times \ldots \times 2 \times 1 = 4 \times 10^{26}$ different possible keys.

- This is too many for a conventional computer to search through in a reasonable amount of time.

But people solve these puzzles while sitting on the beach!

- Commonly occurring letters and letter patterns in English (e.g., ‘E’, ‘T’, ‘A’, ‘O’, ‘TH’) match commonly occurring patterns in the ciphertext.
- Once you get a few parts of the key correct, you can use this knowledge to determine more of the key.
- Secure cryptographic systems have to avoid these pitfalls.

Modern Cryptographic Systems

- Typically the plaintext message is broken up into 128-bit blocks.
- The shared secret key is also 128 bits long. This means there are 2^{128} or about 10^{42} possible different keys.
- Very intricate encryption algorithm: Every bit of the ciphertext block depends on every bit of the plaintext block and every bit of the key.

Simple Substitution Cipher

Key:

```
abcdefghijklmnopqrstuvwxyz
zptrudqmglfnxkaycvejlsowbh
```

Plaintext:

fourscore and seven years ago

Ciphertext:

dalvetavu…….

Modern Cipher

Key:

```
0110110010010101
0100101000010101
0100100100100100
1010100011110010
0100100111000011
1001110001000100
1111000101000100
```

Plaintext:

```
1000111100100101
0101001010000101
0101001110010010
0101010001111001
0010010011100001
1100101100100010
0111100010100010
```

Ciphertext:

```
1000111100100101
0101001010000101
0101001110010010
0101010001111001
0010010011100001
1100101100100010
0111100010100010
```

All bits of key and plaintext are used to compute each bit of ciphertext.

So Bob and Alice can communicate securely

BOB

*Skdn9(&*osaj.v,420kja*

$%^*J<}++UUY

BG&98JIJ I7656><J^%+{'}*

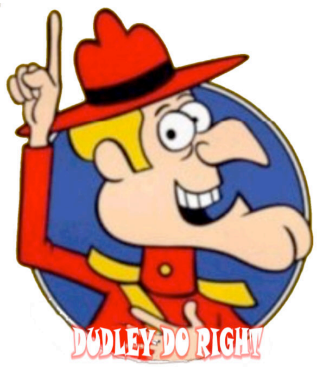
SNIDELY

Curses! Foiled again!

ALICE

Wait a Second

How do Alice and Bob agree on a key in the first place?



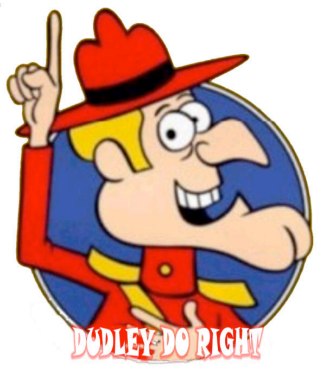
BOB

Nyeh-heh-heh!

SNIDELY

ALICE

If Alice sends the key to Bob over their network connection, Snidely will be able to decrypt all their subsequent communication. Sending it by some other means (Snail mail? Armored car?) is slow and expensive and makes it difficult to change keys, which should be done often.



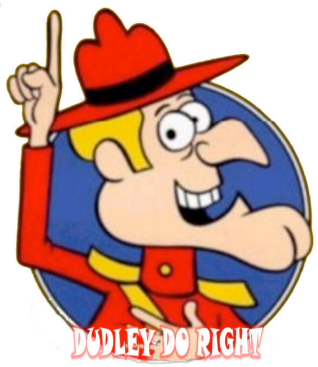
BOB

ALICE

Nyeh-heh-heh!

SNIDELY

Alice might try to encrypt the key with a *second* cipher, but then how do they agree on the key for this new cipher?



BOB

Nyeh-heh-heh!

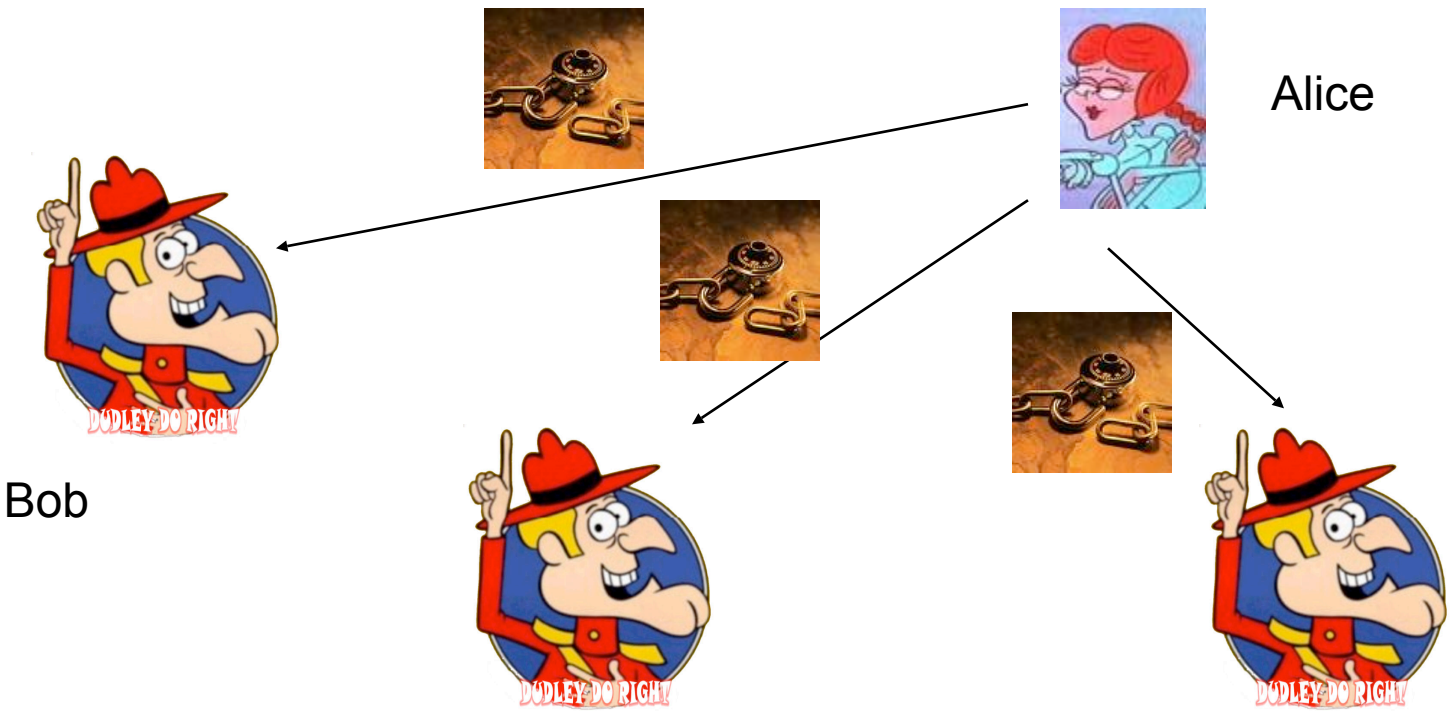
SNIDELY

ALICE

- The *incredible* solution to this key-agreement problem (public-key cryptography) was discovered in the 1970's, independently by academic Computer Scientists and researchers doing classified work for government intelligence agencies.

3. Public-Key Cryptography

Metaphorically….



Alice distributes identical opened combination locks to all of her correspondents. All the locks have the same combination, which she alone knows.

Metaphorically….

Alice

Bob

Rob

Bobby

People sending messages to Alice lock them up in boxes using the combination locks she provided.

Metaphorically….

Curses! Foiled again!

SNIDELY

No matter how closely one examines the lock or tries to reverse-engineer it, it is not possible to figure out the combination.

Literally…

Alice

$K_{private}$

K_{public}

Bob

K_{public}

Rob

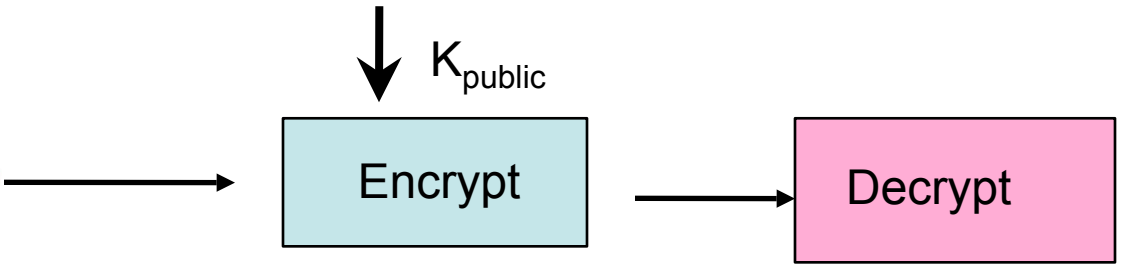
K_{public}

Bobby

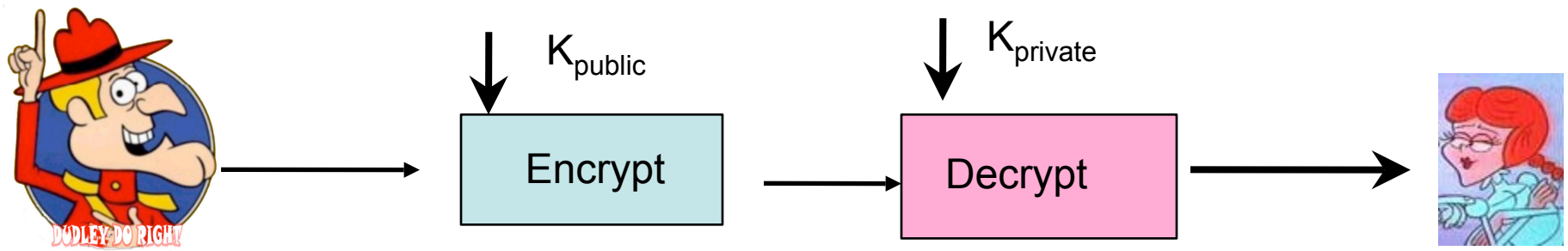
Alice creates two keys—a **public** one that she distributes to all her correspondents…

…and a **private** key that she keeps secret.

Everyone can send Alice an encrypted message, using her public key.

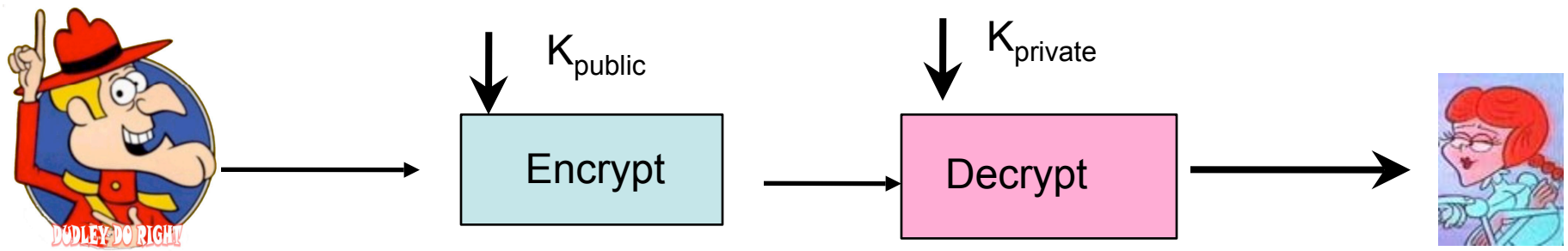


Everyone can send Alice an encrypted message, using her public key.



But only Alice can decrypt, and no amount of inspection of the public key helps to guess the private key. You can't just "reverse the steps" of the encryption algorithm.

Everyone can send Alice an encrypted message, using her public key.



But only Alice can decrypt, and no amount of inspection of the public key helps to guess the private key. You can't just "reverse the steps" of the encryption algorithm.

How is that possible?

This is possible because some problems are much easier to solve in one direction than in the other.

Find two numbers P and Q such that

$P \times Q = 233273$

Find two numbers P and Q such that

P x Q =233273

This is *hard.* To solve this, you might systematically try out candidate divisors: 3,5,7,9, etc. It

What if you were asked the opposite question?

Find 479x487.

This is *easy.* It can be done by hand in a minute or two---it requires nine separate consultations of the multiplication tables, and a similar number of additions of one-digit

Find 479x487.

Multiplying two one hundred-digit numbers to find their two hundred-digit product requires ten thousand consultations of the multiplication table. If you're really bored (or really boring) you can do it by hand in a few days. For a computer, it's a snap.

35324619344027701212726049781984643686711974001976250236493034687761212536794232000585479565280883496

×

7925869954478333033347085841480059687737975857364219960734330341455767872818152135381409304740185467

=

2799783391122132787082946763872260162107044678695542853756000992932612840010760934567105295536085606182235191095136578863710595448200657677509858055761357909873495014417886317894629518723786922182398 3

But *factoring* a 200-digit number into its one hundred-digit factors is at the very limit of what present day computers can do. Factoring a 300-digit number is completely out of reach (like the difference between writing a googol and counting to a googol).

35324619344027701212726049781984643686711974001976250236493034687761212536794232000585479565280883496

×

7925869954478333033347085841480059687737975857364219960734330341455767872818152135381409304740185467

=

2799783391122132787082946763872260162107044678695542853756000992932612840010760934567105295536085606182235191095136578863710595448200657677509858055761357909873495014417886317894629518723786922182398 3

In fact, the number displayed here is the largest ever factored. It took 75 years of computer time.

This is what's behind at least one commonly used public key cryptosystem (RSA).

Alice generates two large (about 1000 bits each) prime numbers P and Q and sends N=PxQ to her correspondents, including Bob.

Bob uses N to encrypt a message sent to Alice (technical details omitted!)

Only someone who knows the factors P and Q can decrypt the message.

What really happens when we buy that book

Cryptographic systems in use today employ a mixture of

Bob's Web browser requests Alice's public key from her Website

Alice's website sends the public key N (open combination lock).

Bob's browser creates a conventional secret key K, encrypts it with N, and sends to Alice. (Normal key secured with combination lock.)

Alice decrypts (unlocks the combination lock) to obtain K, and the two parties communicate, encrypting and decrypting their messages with K. The secret key K is used only for this session.

- If they're used correctly (big if!) modern cryptographic systems provide a very high level of security (although we cannot rule out someone discovering a very fancy method for breaking these systems---like a super-duper factoring algorithm).

If they're used correctly (big if!) modern cryptographic systems provide a very high level of security (although we cannot rule out someone discovering a very fancy method for breaking these systems---like a super-duper factoring algorithm).

But there's a lot more to computer security than cryptography!

"Using encryption on the Internet is like using an armored car to deliver credit card information from someone living in a cardboard box to someone living on a park bench."

---Gene Spafford