

ECE750: Usable Security and Privacy

Communicating Securely

Why Johnny Can't Encrypt

Dr. Kami Vaniea,
Electrical and Computer Engineering
kami.vaniea@uwaterloo.ca



UNIVERSITY OF
WATERLOO

FACULTY OF
ENGINEERING



First, something random...

- First 5 minutes we talk about something interesting, often from recent events
- You will not be tested on the 5 minutes part of lecture
- This part of lecture will sometimes not be recorded
- Why do this?
 1. Some students show up late
 2. Reward students who show up on time
 3. Important to see real world examples

Today...

1. Overview of public/private key encryption
2. Cognitive Walkthrough
3. Deep discussion of the paper: Why Johnny Can't Encrypt

Why Johnny Can't Encrypt

Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0

Alma Whitten
*School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213
alma@cs.cmu.edu*

J. D. Tygar¹
*EECS and SIMS
University of California
Berkeley, CA 94720
tygar@cs.berkeley.edu*

Abstract

User errors cause or contribute to most computer security failures, yet user interfaces for security still tend to be clumsy, confusing, or near-nonexistent. Is this simply due to a failure to apply standard user interface design techniques to security? We argue that, on the contrary, effective security requires a different usability standard, and that it will not be achieved through the user interface design techniques appropriate to other types of consumer software.

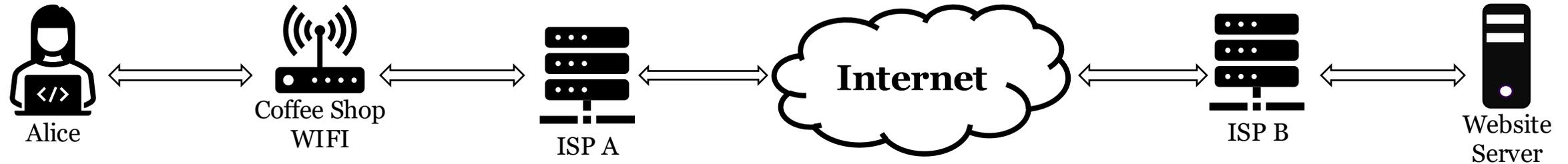
To test this hypothesis, we performed a case study of a security program which does have a good user interface by general standards: PGP 5.0. Our case study used a cognitive walkthrough analysis together with a laboratory user test to evaluate whether PGP 5.0 can be successfully used by cryptography novices to achieve effective electronic mail security. The analysis found a number of user interface design flaws that may

1 Introduction

Security mechanisms are only effective when used correctly. Strong cryptography, provably correct protocols, and bug-free code will not provide security if the people who use the software forget to click on the encrypt button when they need privacy, give up on a communication protocol because they are too confused about which cryptographic keys they need to use, or accidentally configure their access control mechanisms to make their private data world-readable. Problems such as these are already quite serious: at least one researcher [2] has claimed that configuration errors are the probable cause of more than 90% of all computer security failures. Since average citizens are now increasingly encouraged to make use of networked computers for private transactions, the need to make security manageable for even untrained users has become critical [4, 9].

Sample connection: Alice loads a website

Alice visits: `http://example.com`



For each of the above connection points, can they learn:

1. The name and/or IP address of the website Alice is visiting
2. The content of the webpage Alice is viewing
3. Alice's Operating System (Linux, Windows, MacOS)

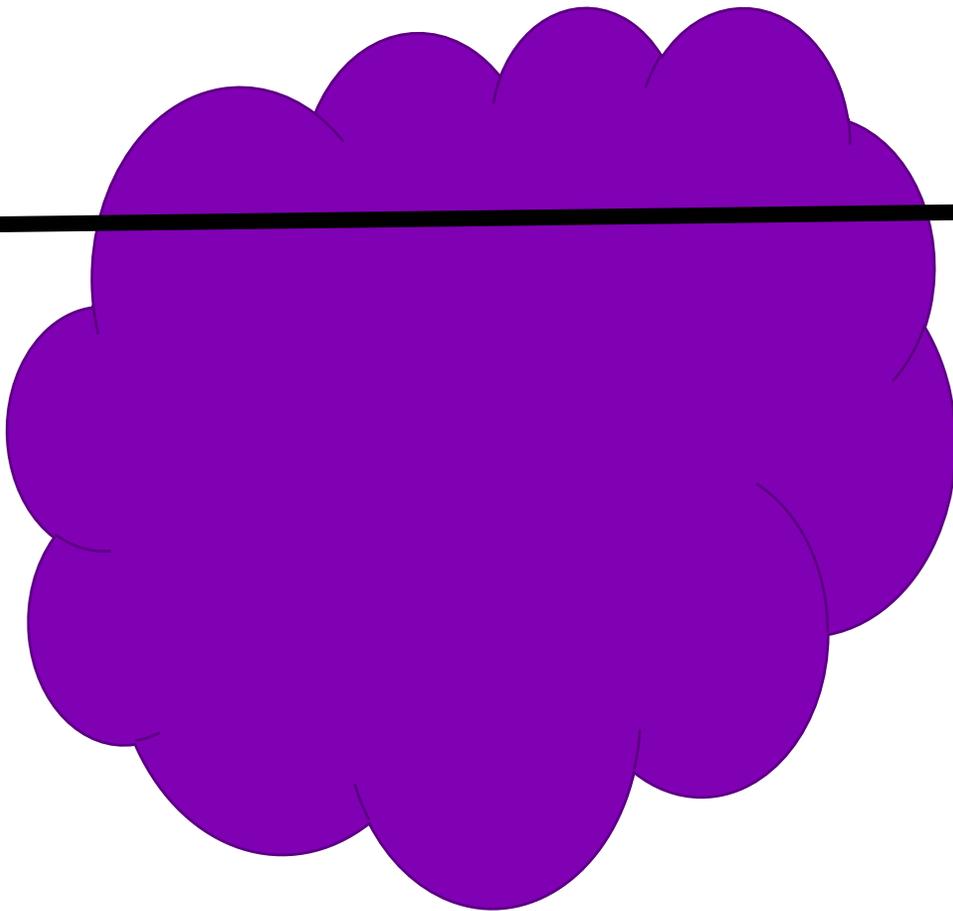
MAN IN THE MIDDLE ATTACK

Alice's
Computer



Alice

The Internet



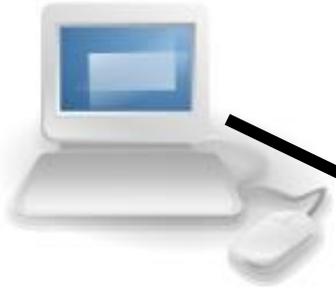
Bob's Server



Bob

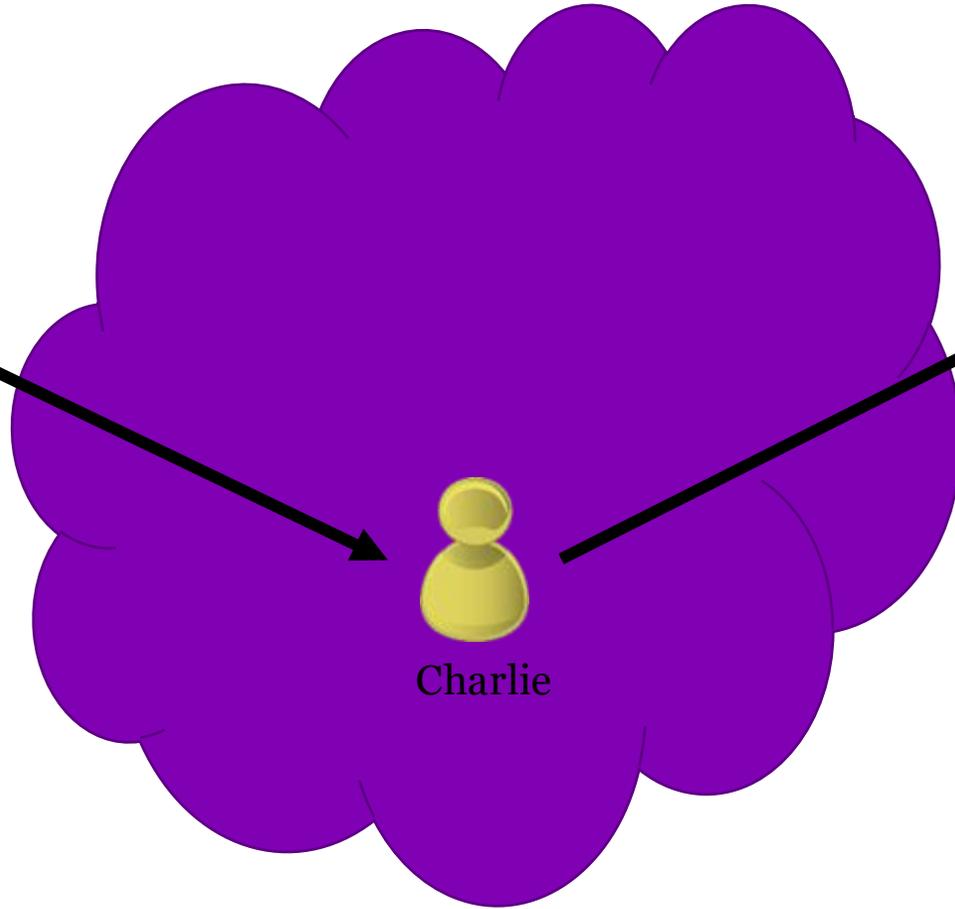


Alice's
Computer



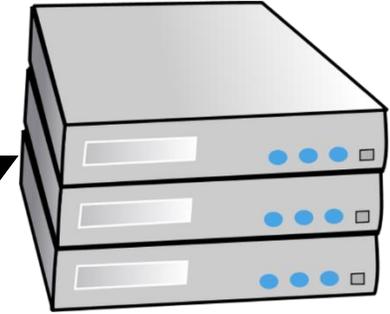
Alice

The Internet

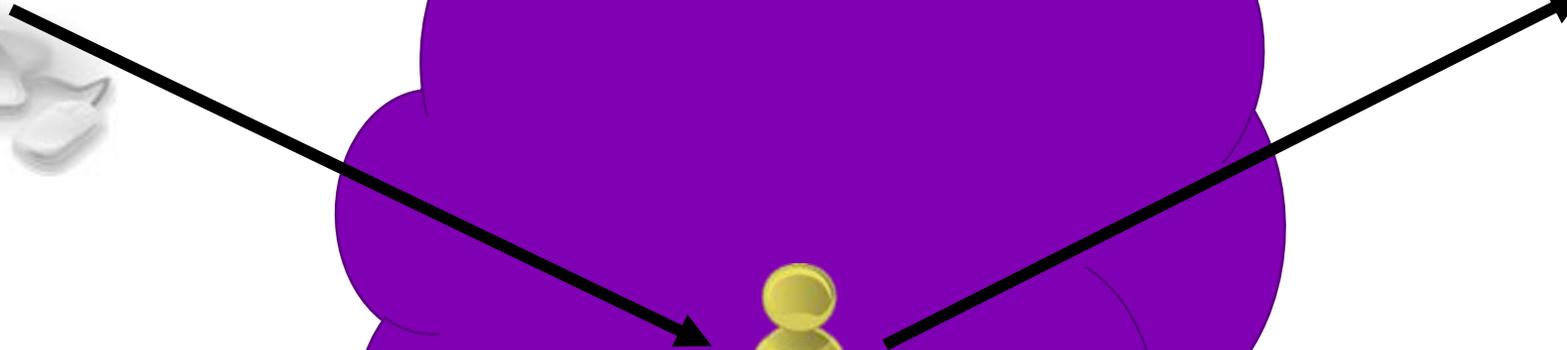


Charlie

Bob's Server



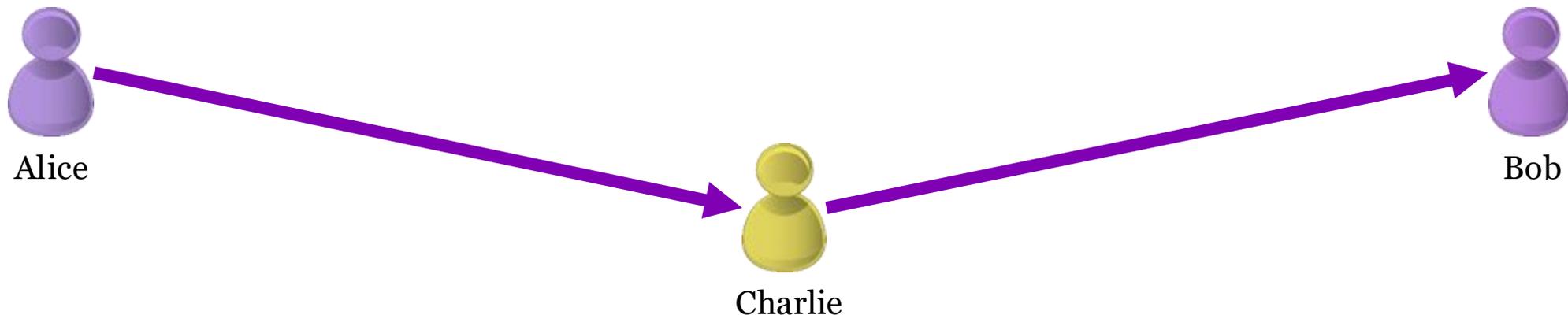
Bob



Charlie is in the middle between Alice and Bob.

- Charlie can:
 - View (confidentiality)
 - Change (integrity)
 - Add (integrity)
 - Delete (integrity, availability)

- Charlie could be:
 - Internet service provider
 - Virtual Private Network (VPN) provider
 - WIFI provider such as a coffee shop
 - An attacker re-routing your connection
 - An incompetent admin (it happens)



Man in the middle attacks happen all the time and they are not always bad.

Alice goes to her favorite coffee shop and tries to visit BBC News



Alice





Alice

The screenshot shows a web browser window with the URL www.bbc.com/news/uk. The page features the BBC logo and navigation menus for News, Sport, and More. The main content area displays the headline "Osborne unveils sugar tax on soft drinks" with a sub-headline: "George Osborne unveils a tax on the makers of soft drinks - and warns of the risks of leaving the EU in his eighth Budget." The article is dated "20 minutes ago" and categorized under "UK Politics". A photograph shows George Osborne speaking in a parliamentary setting. Below the article, there are links for "LIVE Budget 2016 Live" and "Growth forecasts cut", and a video player titled "Budget key points: At-a-glance" with a play button icon and the text "'On course for a surplus'".





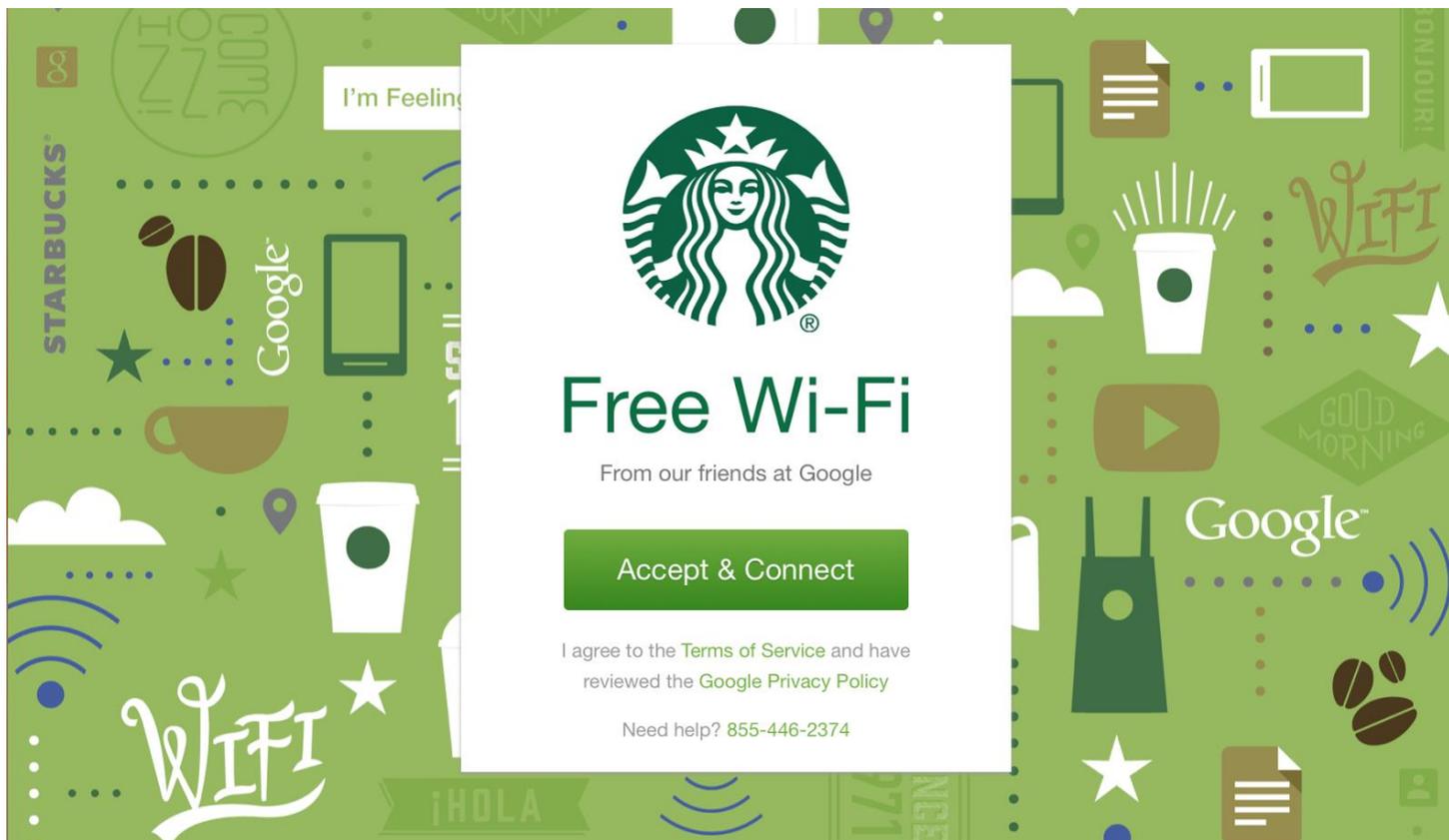
Free Wi-Fi

From our friends at Google

Accept & Connect

I agree to the Terms of Service and have reviewed the Google Privacy Policy

Need help? 855-446-2374

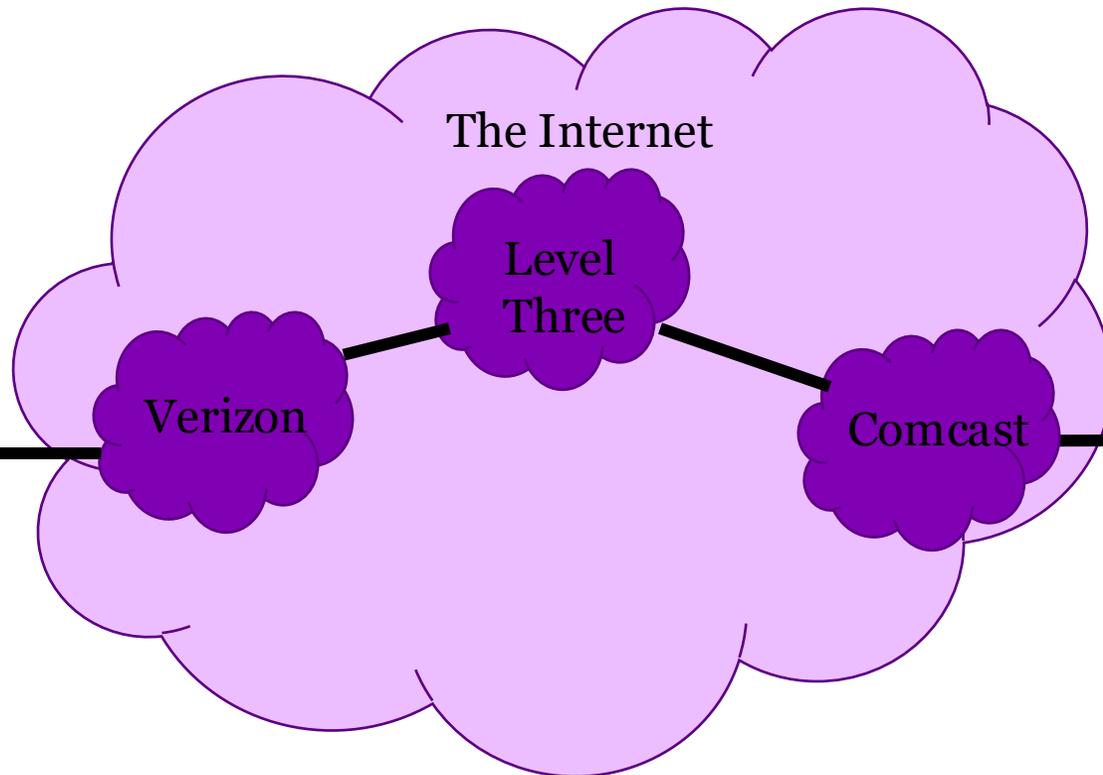




Alice



Your
Computer

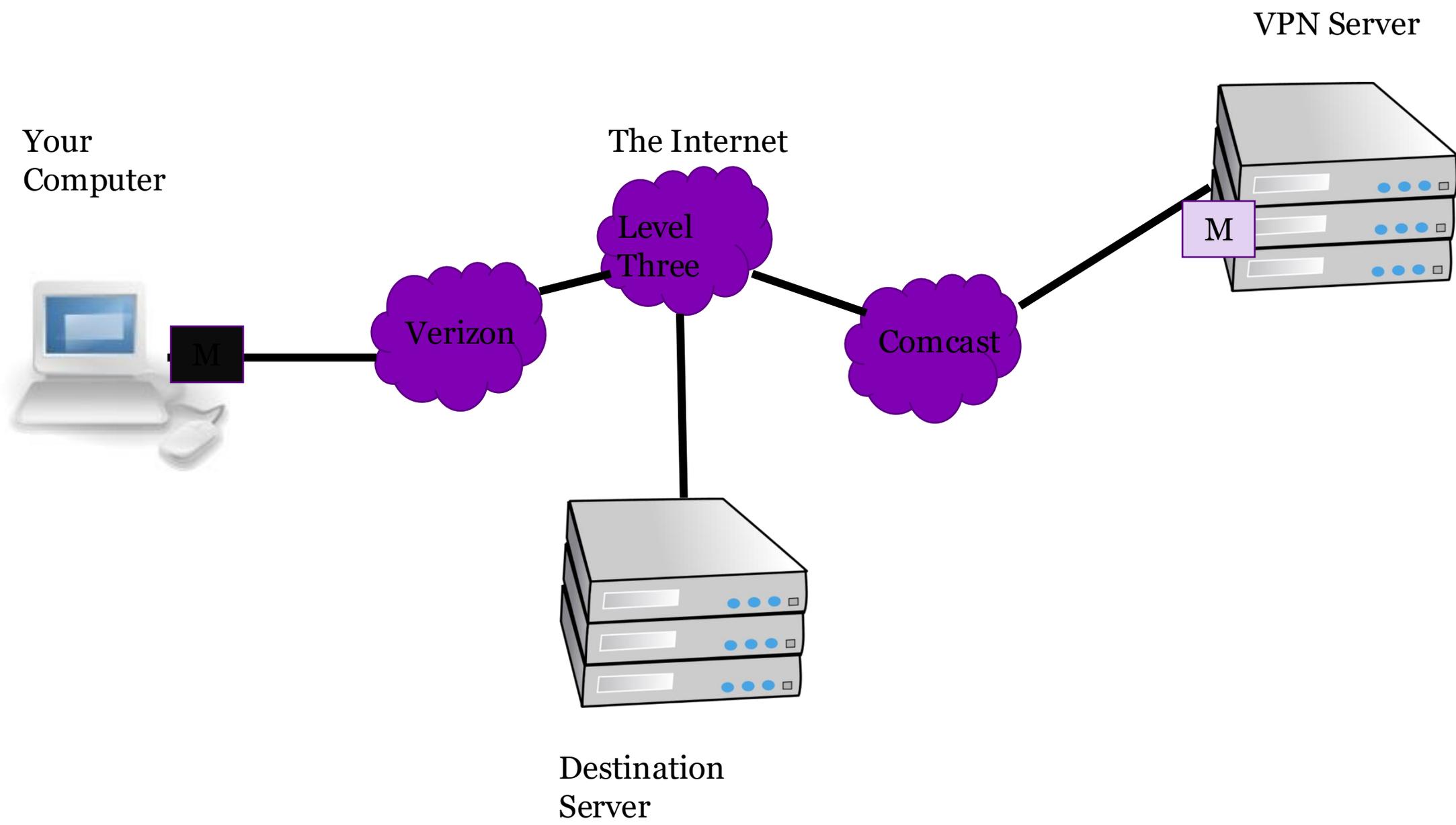


Destination
Server



Virtual Private Networks (VPNs)

Self-inflicted Man in the Middle



Your
Computer

VPN Server

The Internet

Level
Three

Verizon

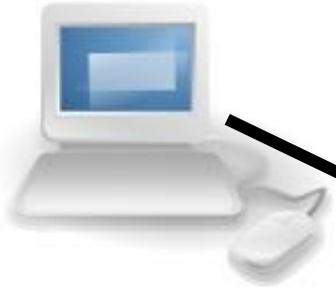
Comcast

M

M

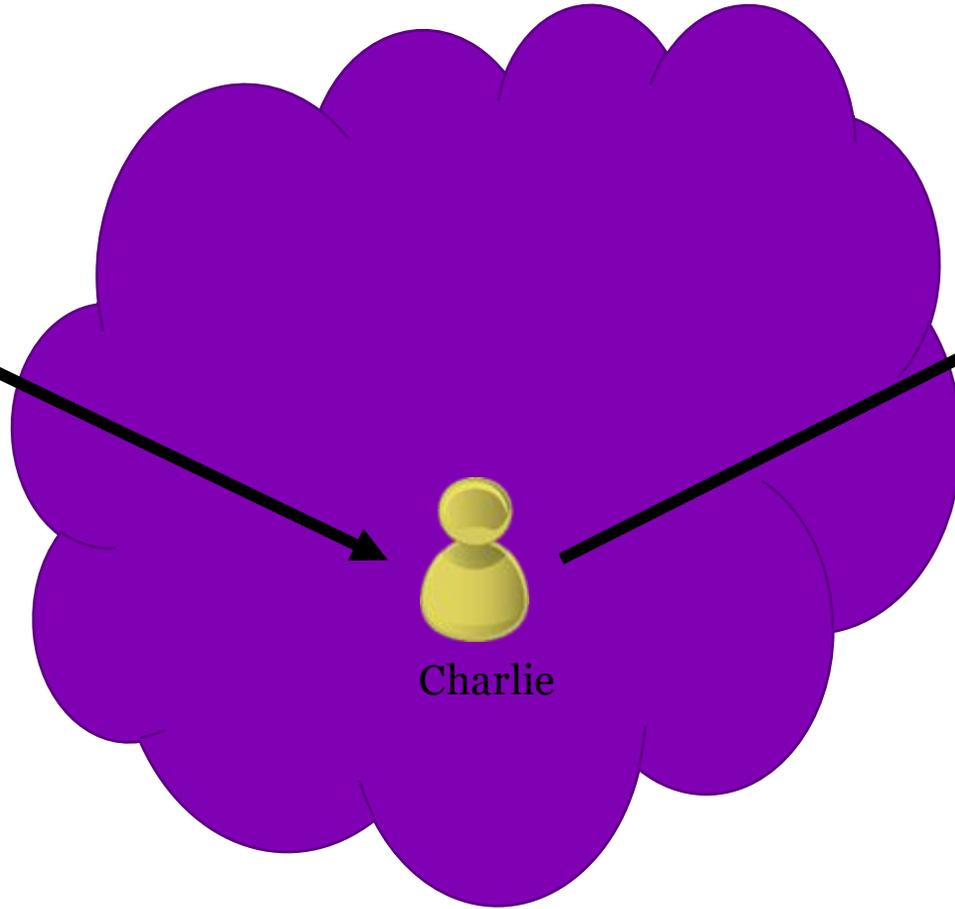
Destination
Server

Alice's
Computer



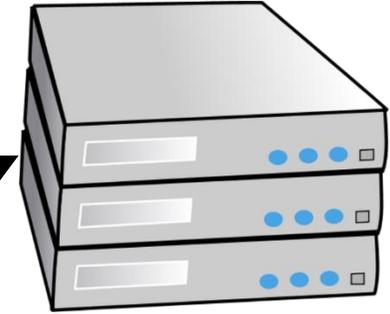
Alice

The Internet

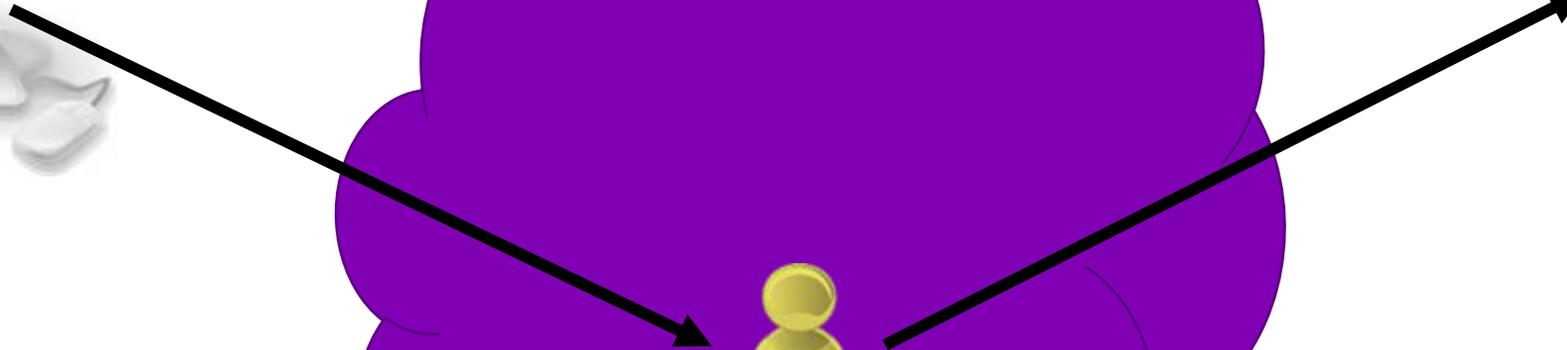


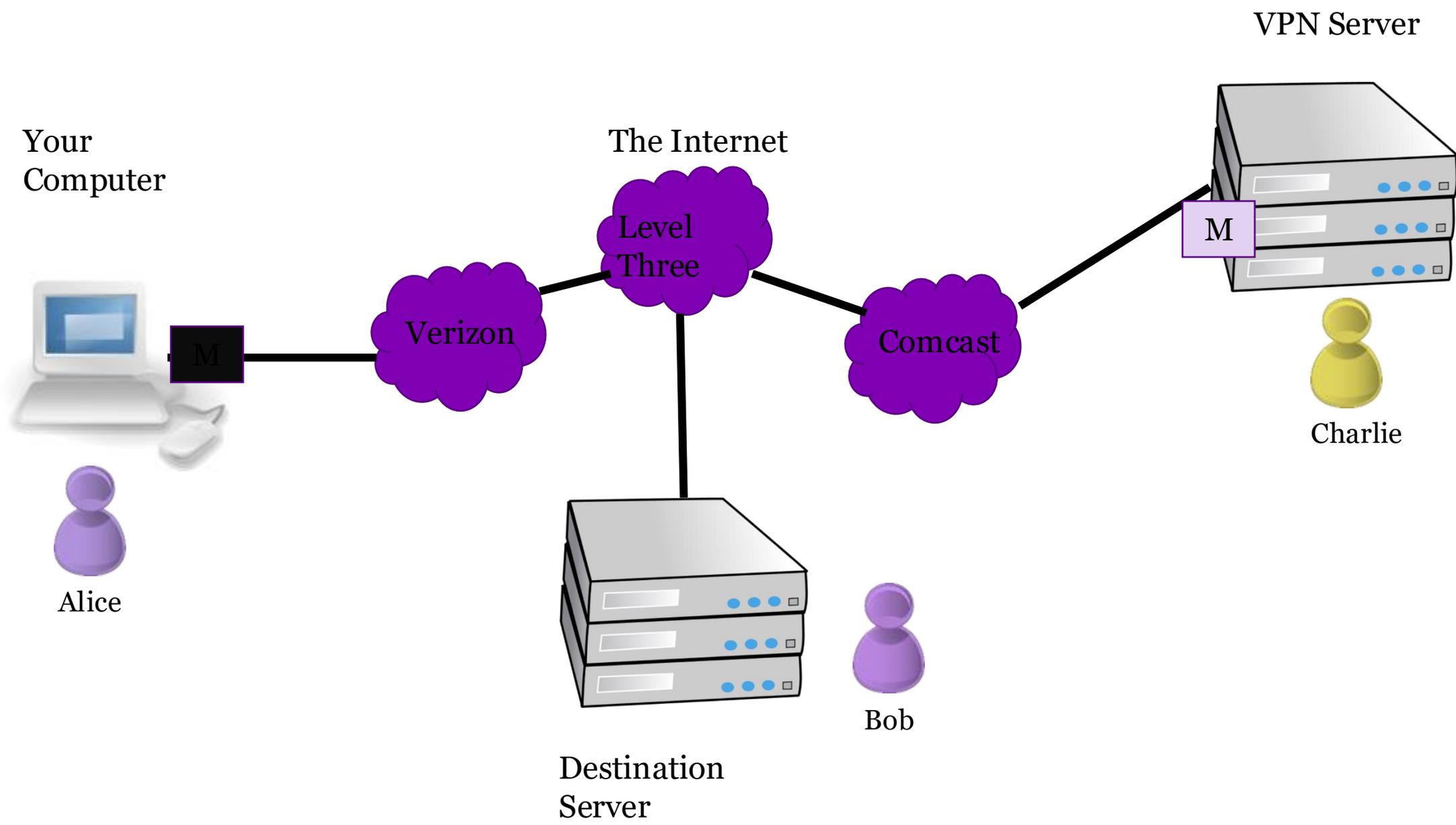
Charlie

Bob's Server



Bob





The following is an attack that actually happened to a student of mine when they were trying to upload their “set a cookie” homework using a free VPN.

```
<html>
<head>
  <title>Basic web page</title>
  <link href="http://vaniea.com/teaching/privacyToday/basic.css" rel="stylesheet" type="text/css"/>
  <script>
    document.cookie="username=John Doe;";
  </script>
</head>
<body>
  THIS TEXT HAS BEEN CHANGED.
</body>
</html>
```

Correct
Answer

```
<html>
<head>
  <title>Basic web page</title>
  <link href="http://vaniea.com/teaching/privacyToday/basic.css" rel="stylesheet" type="text/css"/>
  <script>
    document.cookie="username=John Doe;";
  </script>
</head>
<body>  THIS TEXT HAS BEEN CHANGED.
</body>
</html>
```

Correct
Answer

```
<html>
<head>
  <title>Basic web page</title>
  <link href="http://vaniea.com/teaching/privacyToday/basic.css" rel="stylesheet" type="text/css"/>
  <script>
    document.cookie="username=John Doe;";
  </script>
</head>
<body><script type="text/javascript">ANCHORFREE_VERSION="633161526"</script><script type="text/javascript">var _AF2$ =
{'SN':'HSSHIELDooUS','IP':'216.172.135.223','CH':'HSSCNLoo0550','CT':'z51','HST':'&sessStartTime=1422651433&accessLP=1','AFH':'hss734','RN':Math.floor(Math.random()*999),'TOP':(parent.location!=docum
ent.location||top.location!=document.location)?0:1,'AFVER':'3.42','fbw':false,'FBWCNT':0,'FBWCNTNAME':'FBWCNT_FIREFOX','NOFBWNAME':'NO_FBW_FIREFOX','B':'f','VER':
'us'};if(!_AF2$.TOP==1){document.write("<scr"+"ipt
src='http://box.anchorfree.net/insert/insert.php?sn="+_AF2$.SN+"&ch="+_AF2$.CH+"&v="+ANCHORFREE_VERSION+6+"&b="+_AF2$.B+"&ver="+_AF2$.VER+"&afver="+_AF2$.AFVER+"
type='text/javascript'"></scr"+"ipt">");}</script>
  THIS TEXT HAS BEEN CHANGED.
</body>
</html>
```

Attacked
Answer

```

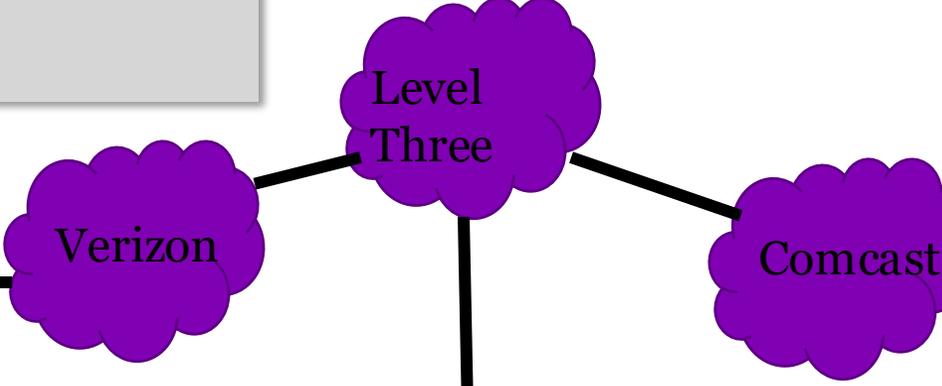
<html>
<head>
  <title>Basic web page</title>
  <link href="http://vaniae.com/teaching/privacyToday/basic.css"
rel="stylesheet" type="text/css"/>
  <script>
    document.cookie="username=John Doe;";
  </script>
</head>
<body>
  THIS TEXT HAS BEEN CHANGED.
</body>
</html>

```

VPN Server



The Internet



Student



Coursework Server

```

<html>
<head>
  <title>Basic web page</title>
  <link href="http://vaniae.com/teaching/privacyToday/basic.css" rel="stylesheet"
type="text/css"/>
  <script>
    document.cookie="username=John Doe;";
  </script>
</head>
<body>
  <script type="text/javascript">ANCHORFREE_VERSION="633161526"</script><
script type='text/javascript'>var _AF2$ =
{'SN':'HSSHIELDooUS','IP':'216.172.135.223','CH':'HSSCNLoo0550','CT':'z5
1','HST':'&sessStartTime=1422651433&accessLP=1','AFH':'hss734','RN':Mat
h.floor(Math.random()*999),TOP:(parent.location!=document.location||to
p.location!=document.location)?0:1,'AFVER':'3.42','fbw':false,'FBWCNT':0,
'FBWCNTNAME':'FBWCNT_FIREFOX','NOFBWNAME':'NO_FBW_FIREF
OX','B':'f','VER':'us'};if(_AF2$.TOP==1){document.write("<scr"+"ipt
src='http://box.anchorfree.net/insert/insert.php?sn="+_AF2$.SN+"&ch="
+_AF2$.CH+"&v="+ANCHORFREE_VERSION+6+"&b="+_AF2$.B+"&ver
="+_AF2$.VER+"&afver="+_AF2$.AFVER+"
type='text/javascript'></scr"+"ipt");}</script>
  THIS TEXT HAS BEEN CHANGED.
</body>
</html>

```

In short:

Dangerous stuff happens on the Internet, do not assume data will be safe in transit

Man in the Middle

Your



The Internet

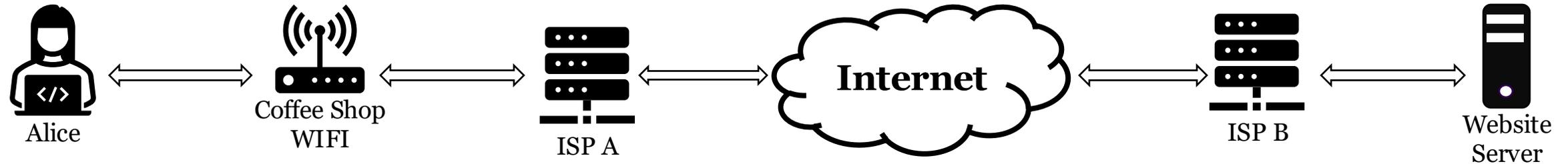


Website Server



Sample connection: Alice loads a website

Alice visits: `http://example.com`



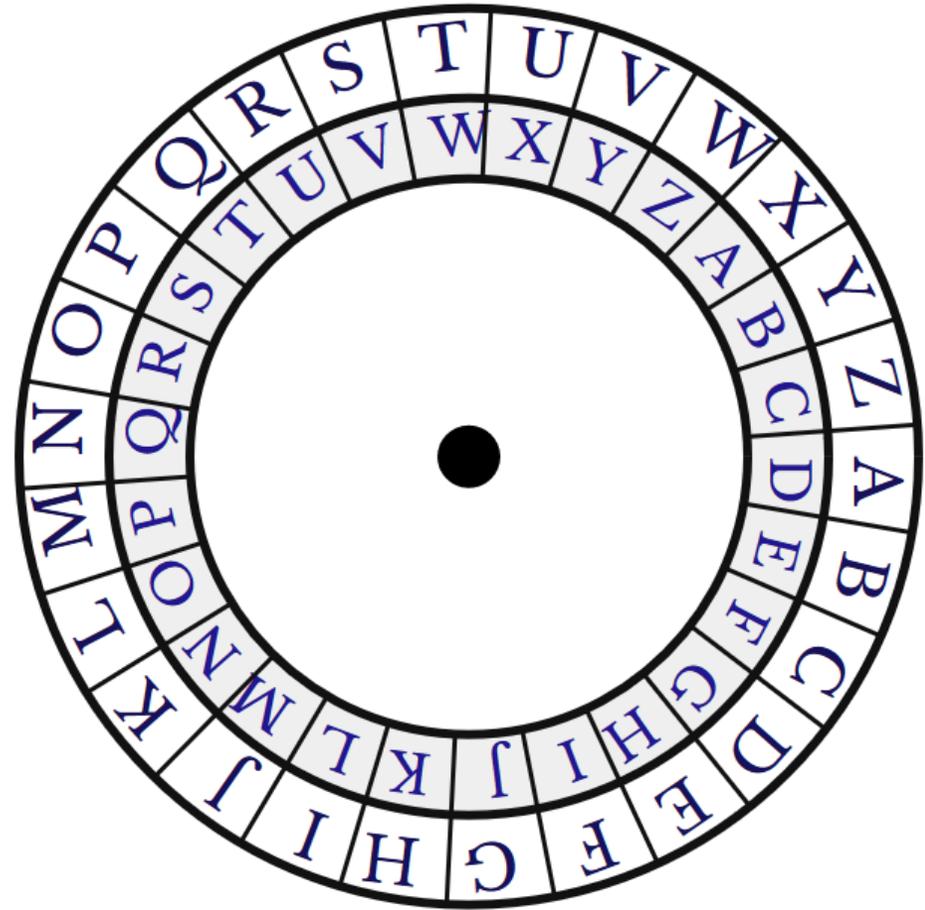
For each of the above connection points, can they learn:

1. The name and/or IP address of the website Alice is visiting
2. The content of the webpage Alice is viewing
3. Alice's Operating System (Linux, Windows, MacOS)

PUBLIC PRIVATE KEY ENCRYPTION

Encryption is based on shared secrets

- In a Caesar Cipher (right) the “secret” is how many places to turn the wheel
- Encryption is done by finding a letter on the outer wheel and then writing down the letter on the inner wheel.
- Easy to break using modern computers by just guessing all 26 possibilities.



Overly simple example using Caesar Cipher with key 3:

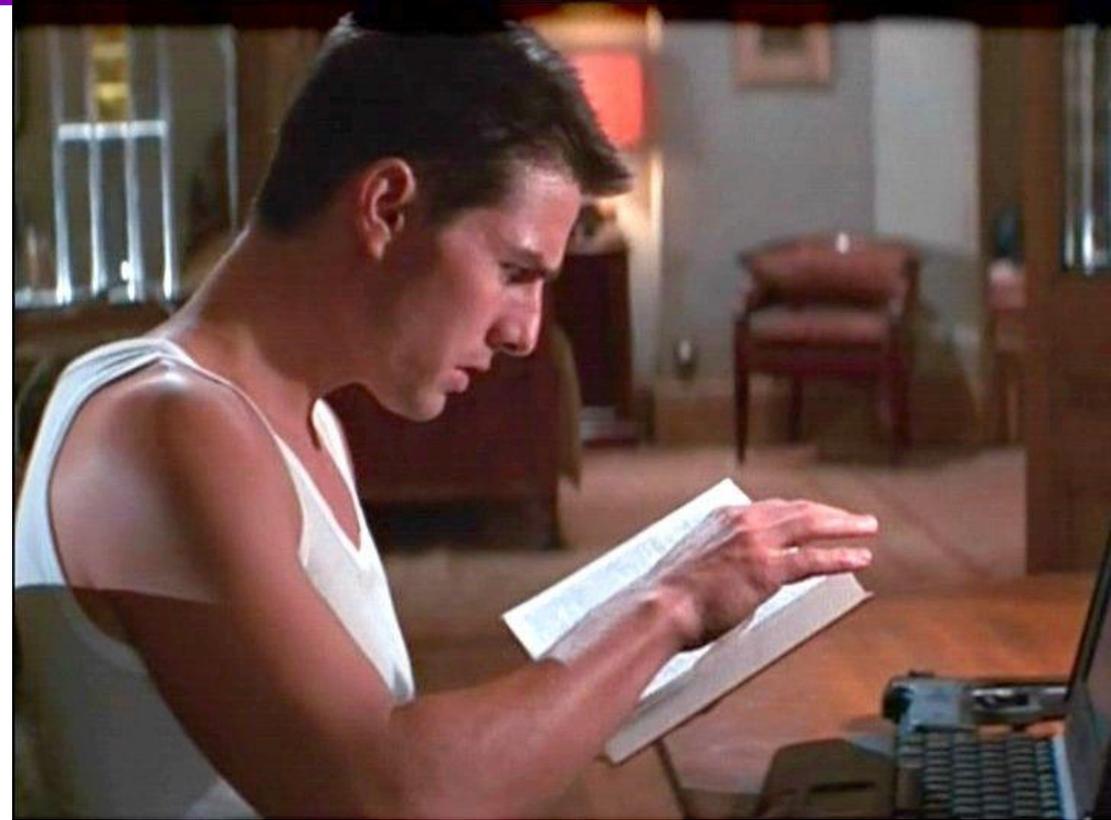
Message	C	R	Y	P	T	O
Encrypted	F	U	V	S	E	R

One-time-pads

- Share a “key” in advance.
- Use the “key” to encrypt/decrypt by adding the letters.
- One of the strongest forms of encryption.
- But... you have to pre-share long keys.

Overly simple example:

Message	C	R	Y	P	T	O
Key	A	Y	S	Y	I	F
Encrypted	C	P	Q	N	B	T



Mission Impossible movie, use of hotel bible as key

Encryption properties we want:

1. The communication between you and the other party is **confidential** and has **not been changed**
 - No one can read what you sent
 - No one can change what you sent
2. **Knowing who** you are communicating with
 - You are talking to who you think you are talking to and not someone else

Public/private key cryptography

- Generate two “keys” that are paired
- **Whatever one key locks only the other key can unlock**



- Public keys are given out to everybody



- Private keys are kept private

My public key



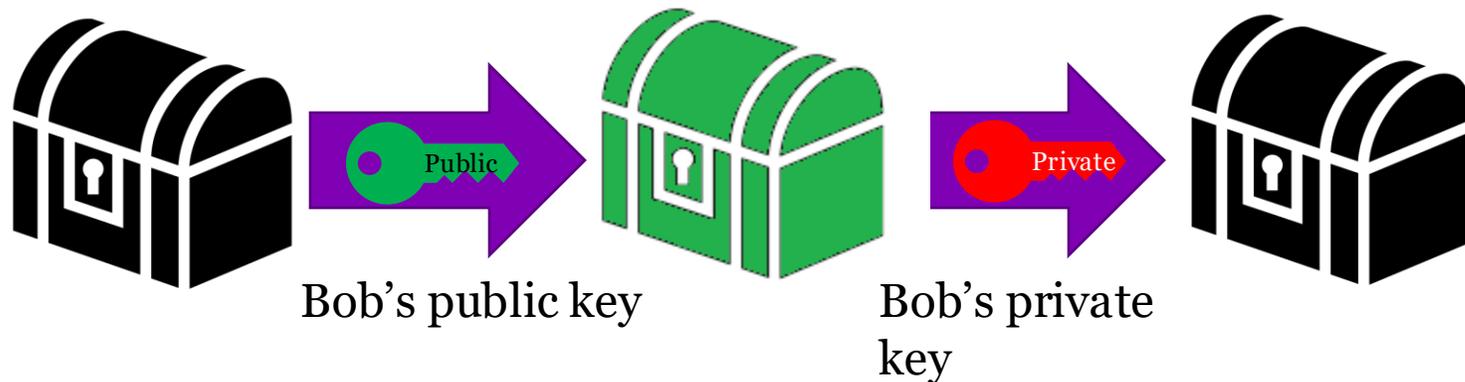
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

```
mQENBFHMcgABCAC9WrYDO6K2L3VHy14eHN6suHLqMpJ+SO+IUTuLEVnUzIoXAUXH
KozHejfv/9XoG8j933ZtszXKCog3aMESeoEoz6fNGfolvaCe5B4jwqoJt8NHwb5L
B2dnqoCplgXcN2GJxFeHHUaf27COsObCjXpMeshU4ZHKke+g6DatmiEtBpVp41Ot
1zgdMqkgb2H2xw28RYfykdDoueteIkOrFLrCy9ZF9KdMhA1eBH94KnwI QshdiZR
QYEX25+M8cKCb++Rc9H6an7EG9WHOFrW40UsY52OfveOyfQPzkkRto7u12339hvHo
B/h+7xLM6FQbOUZQ9BD5w7IQHgytXJVsUjodABEBAAgOIkthbWkgVmFuaVWhIDxr
dmFuaWVhQGluZi5lZC5hYy51az6JAT8EEwELACkFAIYKYvECCGyMFCQlMAYAHcwkI
BwMCAQYVCAIJCgsEFgIDAQIeAQIXgAAKCRCTdSxl9/HZffG+ CACShuKxje3QAqew
GWh8K4gCdiYoxDqJwq3PHxmyhZmQeN/1a1KcOrIj12b+Q75/5t+EgXOHpRoP1xfG
lZ6zOEpf6A18fXx3JgQZdwPDOjtBiWNpOyMeBGTgIvEYg3so2VueQoeXcq3dbYp
5vstVxtD+TKHQ5CioIT75P2bzYq/XLT5aIbNqHQPcTo0DgbRH+FvqsRXr7yeaef
JaPnxXo+1L33t2QY9zctiGyebwrVHMripBJ2VYCDzQk7JuQ5eFh4ZhsMgOmzLQD4
YiGr5weIMFwAvxZOaRxEagVf48jiWvrXuJ8YfHWSohESeNOCYcP8q2oLwwE26T
lpdtrwCqtB1LYW1pIFZhbmlYSA8a2FtaUB2YW5pZWEuY29tPokBQgQTAQIALAIb
IwUJCWYBGAclCQgHAWIBBhULAgkKCwQWAqMBAh4BAheABQJWCmMeAhhBAoJEJN2
zGX38dl9JJAIAIwOrxIYsrnKS6CbW8MgTxxTDOXA Ct1b7FoWoQZHskIUQhEcE+a
XBYibiA5uHaatLfyeXaD3qMEoZnQHoyMGEoGku00wWsbhfoQzHPgwzRLkDii75M
BtbaWwoKWoVB9e4AkMakXJcNf5BXeo6AHRL2v15V2o5DikVnlCRXocKtu8b7LnmK
eLn7oLobr1deIuyKoNzbSnO/vpKDJPo/EY5yUeV9oIypZy/6wFQBegh1sXye6znO
9wb9uUsu9+/P8pz4JILMDSevjfT7zSRSl/YP3fOfZ6N4bc+KODwPM7u510eou9zh
pzibv3ge7VhH2xIWz8vYZ/2xT1345tWRRMOJAhwEEwECAAyFALTnSpEACgkQjyxM
p99tBt2B8A/+OpIzOsQbQJB8yxti4I7PpD1weJdf3a81Vhm7JyXE/Xy66ypfdt3w
XmFRUulrwezYiNebWNCrQHHzQvRv/VJwjbTUx+Q3HsjIkKlHbE7iCiQXXtTRkoEny
2nu dcjGI2vo3C3B2JCucEw6esF1x79PI/IpV2+6tgUBKmDfOpsB2vbtqrHnmAYKL
4lQBfH1YSJgnzwo2JkhhocHdF9oZem1eMeiDeE Vkh63893N8Swk5fBKdJT+SKZ/L
rQEElBBlpMR9BmeY6bPvWRuyevKonIMR8oG9iFABxjTpWBL8aGk6EeVK5EqYDgVkd
ZlarK84r+KU1KD5lfgOCN7nhwgy7VI me68caZHSRiPWZP1fVVMhydiRjv8WsoUs6
InfVU3nxH+ZythPbYot86leGSchBT5K/fBQvbjhrRTbTFwvjzSifb9efWylDi994
nzP6cNOrir3GIpsT8gPGBB2/NjxaWiM6y3X1az1vRnsunQHuyKkFWPZwnEvDJYaC
NN/3jWcbhLFwKBdsA Hp s2+1meFpooJFvNetz2bjT9a9pXaQ6KhOmo5DnhLcaV97
bFBpsUuBGaYZTSSo5x1RdXhqpEbgap8dtuHhVvJw9QYDQBjroK4aKyG9qqMD8cta
Pl/FAdyAqwH8Nw9efqAK+RQxSVUaue9BYEnbIRpsDK6MkP3YMFmu5ki5AQoEUcxy
AAEIALyXYy8G2aTDJpdGcRhmIqOOSUlzPV7/5E5BbYKBNu4KU3nX+JLvcF5jxPQ
42c7i/WRVxE1BJTiarKGSvEvCig4TTXSIUKAt3T1oGBtXmGvqbGBq8ljSGl1UTwdF
5yu5oJyRSf2fqRND6P/2eHNXejDUtdvhUXIU8h9MuUO/ipDoDnwIvMnAATJHA+R
Zqw6oNpyjRGzvr3i uWUwe4PtyJDI3ELAFkbp/NAc5TIuVHRHNOwnpIdJhM5zHuB
QQb3G/EsCn2PQZ5w5SDzavF2SpvQfDqxYpDaTLAXtF+wsJL5iaUjxwRgJPodbCZf
2Tozd7h9MXtGJdIPKJ8eLg8ogcMAEQEAAYkBJQYQAIA DwuUcUxyAAIbDAUJCWYB
gAAKCRCTdSxl9/HZfs+hB/9BJqSmIgcOHFXnb1PVikxekzL8+WVm5Pk/EgMQLSZ2
HX4p3ial5PEPcYgUw9YnaG4ioodwJGw5/daTWrrTzcnKd8YqoP+DUOt96HZDSu3m
mCzE9NVAQYboFbVmGOxoeo627UBSvFqaXvAxBDYkoR8BoTnKhrQFwXkZVb3ohKwD
TgAFjOGIziE6uAdST231tFaqobizYfe5AVXRqro2oxBqNbaJNqs3SWoD83iSyvdv
lloBx83/Rogg7hUkI6F2vzXicWmUwFSXRggCSbLosHsP6isBWwvIHeRmna/aQab
YKG3gbV9iyzAS31gbogVLAZqNSWhp8vVIEE28Fyf/Ed
```

-----END PGP PUBLIC KEY BLOCK-----

I want to send Bob a message that no one else can read

- I encrypt (lock) the message with Bob's public key.
- Only Bob has his private key, so only Bob can decrypt (unlock) the message.



My public key



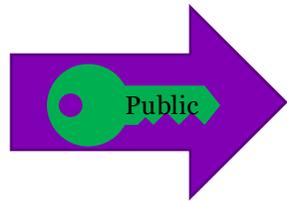
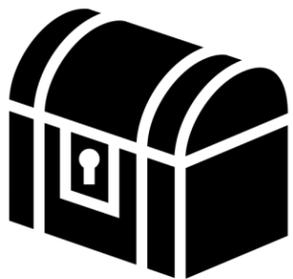
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

```
mQENBFHMcgABCAC9WrYDO6K2L3VHy14eHN6suHLqMpJ+SO+IUTuLEVnUzIoXAUXH  
KozHejFV/9XoG8j933ZtszXKCog3aMESeoEoz6fNGfolvaCe5B4jwqoJt8NHw5L  
B2dnqoCplgXcN2GJxfEHHUaf27COsObCJxPMeshU4ZHke+g6DatmiEBpVp41Ot  
1zgxMqkqb2H2xw28RYfykdDoueteIkOrFlrCy9ZF9KdMhA1eBH94KnwI QshdiZR  
QYEX25+M8cKCb++Rc9H6an7EG9WHOFrW40UsY52OfveOyfQPzkkRto7u12339hvHo  
B/h+7xLM6FQbOUZQ9BD5w7IQHgYtXJVsUjodABEBAAgOIkthbWkgVmFuaVWHIDxr  
dmFuaWVhQGLuZi5jZC5hYy51az6JAT8EEwELACkFAlYKYvECCyMFCQlMAYAHcwkI  
BwMCAQYVCAIJcgsEFgIDAQIeAQIXgAAKCRCTdSxl9/HZffG+ CACShuKxje3QAqew  
GWh8K4gCdiYoxDqJwq3PHxmyhZmQeN/1a1KcOrIj12b+Q75/5t+ EgXOHpRoP IxfG  
LZ6zOEpf6A18fXx3JgQZdwPD0jtBiWNpOyMeBGTgIvEYg3so2VueQoeXcq3dbYp  
5vtVxtD+TKHQ5CioIT75P2bzYq/XLT5aIbNqHQPcToO DgbRH+ FvqsRXr7yeaef  
JaPnxXo+1L33t2QY9zctiGyebwrVHMriPBj2VYCDzQk7uQ5eFh4ZhsMgOmzLQD4  
YiGr5weIMFwAvxZOaRxEagVf48jIwVrxuJ8YfHWSohESeNOCYc2P8q2oLjwwE26T  
lpdtrwCqtB1LYW1pIFZhbmllySA8a2FtaUB2YW5pZWEuY29tPokBQgQTAQIALAIb  
IwUJCWYBgAcLCQgHAWIBBhULAgkKCwQWAqMBAh4BAheABQJWCmMeAhhBAAoJEJN2  
zGX38dl9JJAIAIWorxIYsrnKS6CbW8MgTxxTDOXA Ct1b7FoWoQZHskIUQhEcE+a  
XBiyiA5uHaatLfyjeXaD3qMEoZnQHoyMGEoGKu00wWsbhfoQzHPgwzRLkDii75M  
B1bawwoKWoVB9e4AkMakXJcNf5BXe06AHRL2v15V205DikVnlCRXocKtu8b7LnmK  
eLn7oLobr1deIuyKoNzbSnO/vpKDjPo/EY5yUeV9oIypZy/6wFQBehg1sXye6znO  
9wb9uUsu9+/P8pz4JILMDSevjfT7zSRSl/YP3fOfZ6N4bc+KODwPM7u5Iyoeu9zh  
pzibv3ge7VhH2xIWz8vYZ/2xT1345tWRRMOJAhweEwECAAyFALTnSpEACgkQjyxM  
p99tBt2B8A/+OpIzOsQbQJB8yxti4I7PpD1weJdf3a81Vhm7JyXE/Xy66ypfdt3w  
XmFRUulrwezYiNebWNCrQHHzQvRv/VJwjbTUx+Q3HsjIkKlHbE7iCiQXXtTRkoEny  
2nu dcjGI2vo3C3B2JCucEw6esF1x79PI/Pv2+6tgUBKmDfOpsB2vbtqrHnmAYKL  
4lQBfH1YSJgnzwo2JkhhcHdF9oZem1eMeiDeeVkh63893N8Swk5fBKdTj+SKZ/L  
rQElBBlpMR9BmeY6bPvWRuycVKonIMR8oG9iFABxjTpWBL8aGk6EeVK5EqYDgVkd  
ZlarK84r+KU1KD5IfgOCN7nhwgy7VI me68caZHSRiPWZP1fVVMhydiRjv8WsoUs6  
InfVU3nxH+ZYthPbYot86leGSchBT5K/fBQvbjhrRTbTFwvjzSifb9efWylDi994  
nzP6eNorir3GIpsT8gPgbB2/NjxaWiM6y3X1az1vRnsunQHuyKkFWPZwnEvDJYaC  
NN/3jWcbhLFwKBdsA Hps2+1meFPooJFvNetz2bjT9a9pXaQ6KhOm5DnhLcaV97  
bFBpsUuBGaYZTSSo5x1RdXhqpEbgap8dtuHhVvJw9QYDQBjroK4aKyG9qqMD8cta  
Pl/FAdyAqwH8Nw9efqAK+RQxSVUae9BYEnbIRpsDK6Mkp3YMFmu5ki5AQoEUcxy  
AAEIALyXYy8G2aZTDJpdGeRhmIqOOSUlzPV7/5E5BbYKBNu4KU3nX+JLvcF5jxPQ  
42c7i/WRVxE1BJTiarKgsEvC94TTXSIUKAt3T1oGBtXmGvqbGBq8ljSGl1UTwdf  
5yu5oJyRSf2fqRND6P/2eHNXejDUtdvhUXIUt8h9MuUO/ipDoDnWlVmnAatJHA+R  
Zqw6oNpyjRgzv3iUWu4PtyJDI3ELAFkpb/NAc5TIuVHRHNOwNpldJhM5zHuB  
QQb3G/EsCn2PQZ5w5SDzavF2SpvQfDqxYpDaTLAXiF+wsJL5iaUjxwRgJPoDbCZf  
2Tozd7h9MXtGJdIPKJ8eLG8ogcMAEQEAAYkBJQYQAQIADwUCUcxyAAiBDAUJCWYB  
gAAKCRCTdSxl9/HZfs+hB/9BJqSmIgcoHFXnbiPVIKxekzL8+WVw5Pk/EgMQSLZ2  
HX4p3ial5PEPEyGUw9YnaG4ioodwJGw5/dATWRrTzenJGw5/dATWRrTzenKd8YqoP+DUOt96HZDSu3m  
CxE9NVAQYboFvBmGOXoeo627UBSvFqaXvAXBDYkoR8BoTnKhrQTFvXkZVb3ohKwD  
TgAFjOGIZiE6uAdST231tFaqobizYfe5AVXRqro2oxBqNbaJNqs3SWoD83iSyvdv  
lloBx83/Rogg7hUk16F2vzXicWmUwFSXRggCSbLosHsP6isBWwvIHeRmna/aQab  
YKG3gbV9iyzAS31gbogVLAZqNSWhp8vVIEE28Fyf/Ed
```

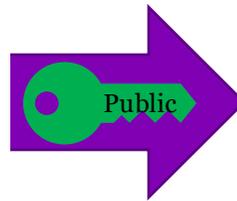
-----END PGP PUBLIC KEY BLOCK-----

I want to send Bob a message that no one else can read

- I encrypt (lock) the message with Bob's public key.
- Only Bob has his private key, so only Bob can decrypt (unlock) the message.
- Using the same key twice just creates an error (meaningless output)



Bob's public key



Bob's public key

Error

My public key



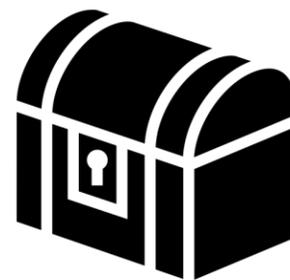
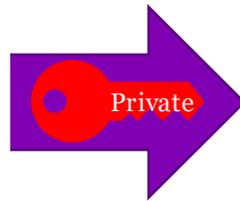
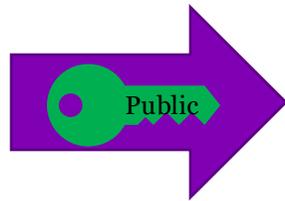
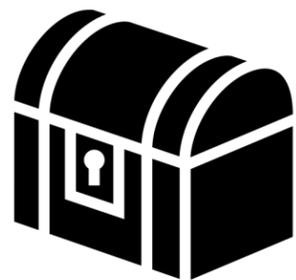
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

```
mQENBFHMCGABCAC9WrYDO6K2L3VHy14eHN6suHLqMpJ+SO+IUTuLEVnUzIoXAUXH  
KozHejFV/9XoG8j933ZtsXKCog3aMESeoEoz6fNGfolvaCe5B4jwqoJt8NHwb5L  
B2dnqoCplgXcN2GJxfEHHUaf27COSobCjXpMeshU4ZHKke+g6DatmiEBpVp41Ot  
1zgxndMQkgb2H2xw28RYfykdDoueteIkOrFlrCy9ZF9KdMhA1eBH94KnwI QshdiZR  
QYEX25+M8cKCb++Rc9H6an7EG9WHOFrW40UsY52OfveOyfQPzkkRto7u12339hvHo  
B/h+7xLM6FQbOUZQ9BD5w7IQHgYtXJVsUjodABEBAAgOIkthbWkgVmFuaVWHIDxr  
dmFuaWVhQGLuZi5jZC5hYy51az6JAT8EEwELACkFAlYKYvECCgYMFCQlMAYAHcWkI  
BwMCAQYVCAIJcgsEFgIDAQIEAQIXgAAKCRCTdSxl9/HZffG+CACShuKxje3QAqew  
GWh8K4gCdiYoxDqJwq3PHxmyhZmQeN/1a1KcOrIj12b+Q75/5t+EgXOHpRoP1xfG  
LZ6zOEpf6A18fXx3JgQZdwPD0jtBiWNpOyMeBGTgIvEYg3so2VueQoeXcq3dbYp  
5vstVxtD+TKHQ5CioIT75P2bzYq/XLT5aIbNqHQPcToOdgBRH+FvqsRXr7yeaef  
JaPnxXo+1L33t2QY9zctiGyebwrVHMriPBj2VYCDzQk7uQ5eFh4ZhsMgOmzLQD4  
YiGr5weIMFwAvxZOaRxEagVf48jiWvrXuJ8YfHWSohESeNOCYc2P8q2olJwwE26T  
lpdtrwCqtB1LYW1pIFZhbmllySA8a2FtaUB2Yw5pZWEuY29tPokBQgQTAQIALAIb  
IwUJCWYBgAcLcQgHAWIBBHUIAgkKCwQWAqMBAh4BAheABQJWcmMeAhkBAaOJEJN2  
zGX38dl9JJAIAIWorxIYsrnKS6CbW8MgTxxTDOXaCt1b7FoWoQZHskIUQhEcE+a  
XBiyiA5uHaatLfyjeXaD3qMEoZnQHoYMGEoGKu00wWsbhfoQzHPgwzRLkDii75M  
B1bawwoKWoVB9e4AkMakXJcNf5BXe06AHL2v15V205DikVnlCRXocKtu8b7LnmK  
eLn7oLobr1deIuyKoNzbSnO/vpKDjpo/EY5yUeV9oIypZy/6wFQBehg1sXye6znO  
9wb9uUsu9+/P8pz4JILMDSevjfT7zSRSl/YP3fOfZ6N4bc+KODwPM7u5Iyoeu9zh  
pzibv3ge7VhH2xIWz8vYZ/2xT1345tWRRMOJAhweEwECAAyFALTnSpEACgkQjyxM  
p99tBt2B8A/+OpIzOsQbQJB8yxti4I7PpD1weJdf3a81Vhm7JyXE/Xy66ypfdt3w  
XmFRUulrwezYInebWNCrQHzQvRv/VJwjbTUX+Q3HsjIkKlHbE7iCiQXxtTRkoEny  
2nuDcJGI2vo3C3B2JCucEw6esF1x79PI/IpV2+6tgUBKmDfOpsB2vbtqrHnmAYKL  
4lQBfH1YSJgnzwo2JkhhocHdF9oZem1eMeiDeeVkh63893N8Swk5fBKdTj+SKZ/L  
rQEElBBlpMR9BmeY6bPvWRuyevKonIMR8oG9iFABXjTpWBL8aGk6EeVK5EqYDgVkd  
ZlarK84r+KU1KD5lfgOCN7nhwgy7VI me68caZHSRiPWZP1fVVMhydiRjv8WsoUs6  
InfVU3nxH+ZYthPbYot86leGSchBT5K/fBQvbjhrRTbTFwvjzSifb9efWylDi994  
nzP6eNorir3GIpsT8gPGBB2/NjxaWiM6y3X1az1vRnsunQHuyKkFWPZwnEvDJYaC  
NN/3jWcbhLFwKBDSaHpS2+1meFPooJFvNetz2bjT9a9pXaQ6KhOmo5DnhLcaV97  
bFBpsUuBGaYZTSSo5x1RdXhqpEbgap8dtuHhVvJw9QYDQBjroK4aKyG9qqMD8cta  
Pl/FAdyAqwH8Nw9efqAK+RQxSVUae9BYEnbIRpsDK6Mkp3YMFmu5ki5AQoEUcxy  
AAEIALyXYy8G2ZaTdJpdGcRhmIqOOSUlzPV7/5E5BbYKBNu4KU3nX+JLvcF5jxPQ  
42c7i/WRVxE1BJTiarKGSvEvC94TTXSIUKAt3T1oGBtXmGvqbGBq8ljSGl1UTwdf  
5yu5oJyRSf2fqRND6P/2eHNXjeDUdvhUXIU8h9MuUO/ipDoDnwlVmnAATJHA+R  
Zqw6oNpyjRGzvr3iUWu4PtyJDI3ELAFkpb/NAc5TIuVHRHNOwnpldJhM5zHuB  
QQb3G/EsCn2PQZ5w5SDzavF2SpvQfDqxYpDaTLAXiF+wsJL5iaUjxwRgJPodbCZf  
2Tozd7h9MXtGJdIPKJ8eLG8ogcMAEQEAAYkBJQYQAIA DWUCUcxyAAIbDAUJCWYB  
gAAKCRCTdSxl9/HZfs+hB/9BJqSmIgcOHFXnbiPVikxekzL8+VWm5Pk/EgMQSLZ2  
HX4p3ial5PEPcYgUw9YnaG4ioodwJGw5/daTWrrTznKd8YqoP+DUOt96HZDSu3m  
mCzE9NVAQYboFbVmGOXoeo627UBSvFqaXvAxBDYkoR8BoTnKhrQfVXkZVb3ohKwD  
TgAFjOGIziE6uAdST231tFaqobizYfe5AVXRqro2oxBqNbaJNqs3SWoD83iSyvdv  
lIOBx83/Rogg7hUkI6F2vzXicWmUwFSXRggCSbLosHsP6isBWwvIHeRmna/aQab  
YK3g3bV9jyczAS31gbogVLAZqNSWhp8vVIEE28Fyf/Ed
```

-----END PGP PUBLIC KEY BLOCK-----

I want to send Bob a message that no one else can read

- I encrypt (lock) the message with Bob's public key.
- Only Bob has his private key, so only Bob can decrypt (unlock) the message.



Bob's public key

Bob's private key

My public key



-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

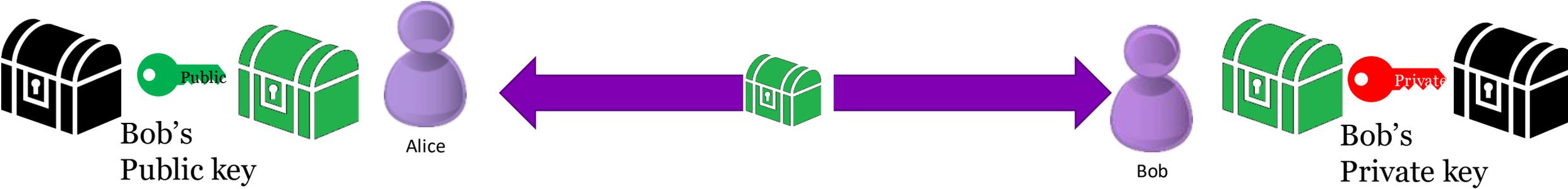
```
mQENBFHMcgABCAC9WrYDO6K2L3VHy14eHN6suHLqMpJ+SO+IUTuLEVnUzIoXAUXH  
KozHejFV/9XoG8j933ZtszXKCog3aMESeoEoz6fNGfolvaCe5B4jwqoJt8NHw5L  
B2dnqoCplgXcN2GJxfEHHUaf27COsObCJxPMeshU4ZHke+g6DatmiEBpVp41Ot  
1zgxMqkqb2H2xw28RYfykdDoueteIkOrFLrCy9ZF9KdMhA1eBH94KnwI QshdiZR  
QYEX25+M8cKCb++Rc9H6an7EG9WHOFRW40UsY52OfveOyfQPzkkRto7u12339hvHo  
B/h+7xLM6FQbOUZQ9BD5w7IQHgYtXJVsUjodABEBAAgOIkthbWkgVmFuaVWHIDxr  
dmFuaWVhQGLuZi5jZC5hYy51az6JAT8EEwELACkFAIYKYvECCyMFCQlMAYAHcWkI  
BwMCAQYVCAIJcgsEFgIDAQIeAQIXgAAKCRCTdSxl9/HZffG+CACShuKxje3QAqew  
GWh8K4gCdiYoxDqJwq3PHxmyhZmQeN/1a1KcOrIj12b+Q75/5t+EgXOHpRoP1xfG  
LZ6zOEpf6A18fXx3JgQZdwPD0jtBiWNpOyMeBGTglvEYg3so2VueQoeXcq3dbYp  
5vtVxtD+TKHQ5CioIT75P2bzYq/XLT5aIbNqHQPcToO DgbRH+FvqsRXr7yeaef  
JaPnxXo+1L33t2QY9zctiGyebwrVHMriPBj2VYCDzQk7uQ5eFh4ZhsMgOmzLQD4  
YiGr5weIMFwAvxZOaRxEagVf48jIwVrxuJ8YfHWSohESeNOCYc2P8q2oLjwwE26T  
lpdtrwCqtB1LYW1pIFZhbmllySA8a2FtaUB2YW5pZWEuY29tPokBQgQTAQIALAIb  
IwUJCWYBgAcLCQgHAWIBBhULAgkKCwQWAqMBAh4BAheABQJWCmMeAhhBAAoJEJN2  
zGX38dl9JJAIAIWorxIYsrnKS6CbW8MgTxxTDOXA Ct1b7FoWoQZHskIUQhEcE+a  
XYyib1A5uHaatLfyjeXaD3qMEoZnQHoyMGEoGKu0oWsbhfoQzHPgwzRLkDii75M  
B1bawwoKWoVB9e4AkMakXJcNf5BXe06AHRL2v15V205DikVnlCRXocKtu8b7LnmK  
eLn7oLobr1deIuyKoNzbSnO/vpKDjPo/EY5yUeV9oIypZy/6wFQBehg1sXye6znO  
9wb9uUsu9+/P8pz4JILMDSevjfT7zSRSl/YP3fOfZ6N4bc+KODwPM7u5Iyoeu9zh  
pzibv3ge7VhH2xIWz8vYZ/2xT1345tWRRMOJAhweEwECAAyFALTnSpEACgkQjyxM  
p99tBt2B8A/+OpIzOsQbQJB8yxti4I7PpD1weJdf3a81Vhm7JyXE/Xy66ypfdt3w  
XmFRUulrwezYiNebWNCrQHHzQvRv/VJwjbTUx+Q3HsjIkKlHbE7iCiQXXtTRkoEny  
2nu dcjGI2vo3C3B2JCucEw6esF1x79PI/IPv2+6tgUBKmDfOpsB2vbtqrHnmAYKL  
4lQBfH1YSJgnzwo2JkhhocHdF9oZem1eMeiDeE Vkh63893N8Swk5fBKdTj+SKZ/L  
rQElBBlpMR9BmeY6bPvWRuycVKonIMR8oG9iFABxjTpWBL8aGk6EeVK5EqYDgVkd  
ZlarK84r+KU1KD5lfgOCN7nhwgy7VI me68caZHSRiPWZP1fVVMhydiRjv8WsoUs6  
InfVU3nxH+ZYthPbYot86leGSchBT5K/fBQvbjhrRTbTFwvjzSifb9efWylDi994  
nzP6eNorir3GIpsT8gPGBB2/NjxaWiM6y3X1az1vRnsunQHuyKkFWPZwnEvDJYaC  
NN/3jWcbhLFwKBdsA Hps2+1meFPooJFvNetz2bjT9a9pXaQ6KhOm5DnhLcaV97  
bFBpsUuBGaYZTSSo5x1RdXhqpEbgap8dtuHhVvJw9QYDQBjroK4aKyG9qqMD8cta  
Pl/FAdyAqwH8Nw9efqAK+RQxSVUae9BYEnbIRpsDK6Mkp3YMFmu5ki5AQoEUcxy  
AAEIALyXYy8G2aZdTJpdGeRhmIqOOSUlzPV7/5E5BbYKBNu4KU3nX+JLvcF5jxPQ  
42c7i/WRVxE1BJTiarKgsEvC94TTXSIUKAt3T1oGBtXmGvqbGBq8ljSGl1UTwdf  
5yu5oJyRSf2fqRND6P/2eHNXejDUtdvhUXIUt8h9MuUO/ipDoDnWlVmnAatJHA+R  
Zqw6oNpyjRGzrv3iUWu4PtyJDI3ELAFkpb/NAc5TIuVHRHNOwNpldJhM5zHuB  
QQb3G/EsCn2PQZ5w5SDzavF2SpvQfdqxYpDaTLAXiF+wsJL5iaUjxwRgJPodbCZf  
2Tozd7h9MXtGJdIPKJ8eLG8ogcMAEQEAAYkBJQYQAQIADwUcUcxyAAiBDAUJCWYB  
gAAKCRCTdSxl9/HZfs+hB/9BJqSmIgcoHFxn1PVIKxekzL8+WVw5Pk/EgMQSLZ2  
HX4p3ial5PEPcYgUw9YnaG4ioodwJGw5/dATWRrTzenJGw5/dATWRrTzenKd8YqoP+DUOt96HZDSu3m  
CzE9NVAQYboFbVmGOxoeo627UBSvFqaXvAvBDYkoR8BoTnKhrQTFvXkZVb3ohKwD  
TgAFjOGIZiE6uAdST231tFaqobizYfe5AVXRqro2oxBqNbaJNqs3SWoD831Syvdv  
lloBx83/Rogg7hUk16F2vzXicWmUwFSXRggCSbLosHsP6isBWwvIHeRmna/aQab  
YKG3gbV9iyzAS31gbogVLAZqNSWhp8vVIEE28Fyf/Ed
```

-----END PGP PUBLIC KEY BLOCK-----

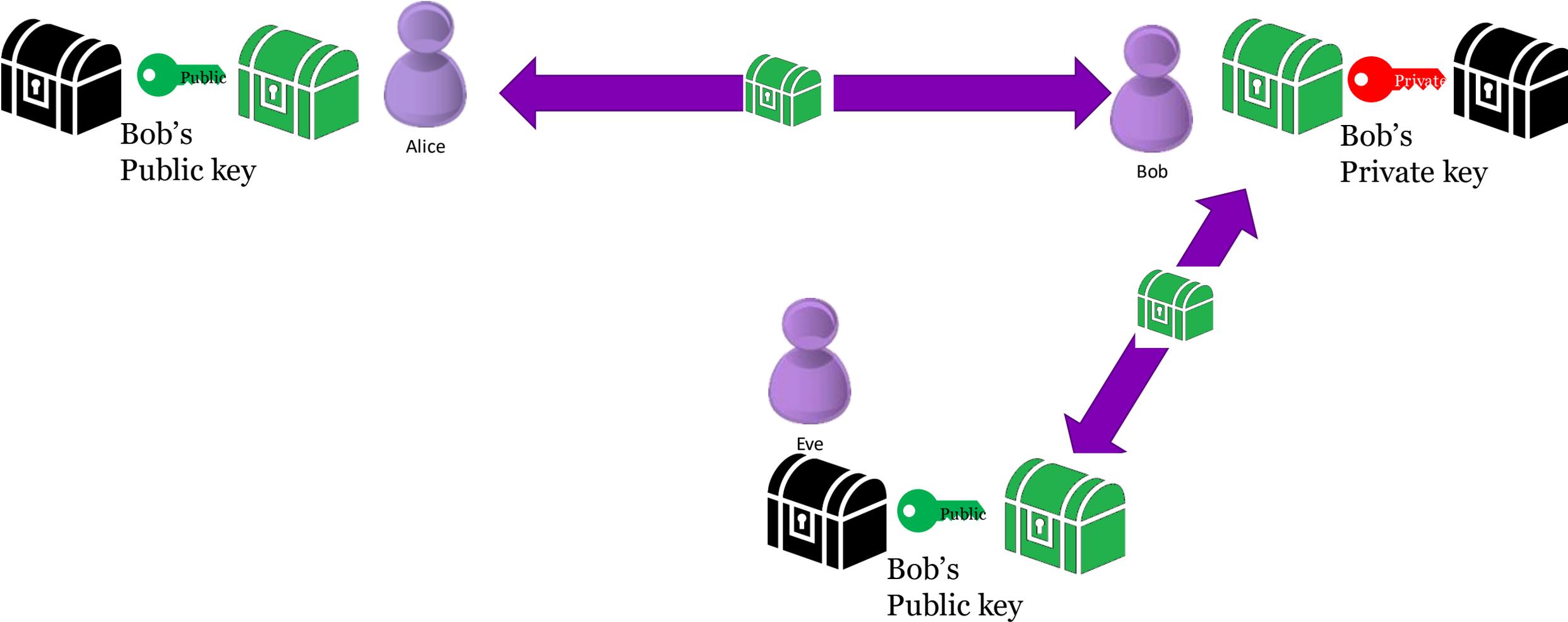
Encryption properties we want:

1. The communication between you and the other party is **confidential** and has **not been changed (integral)**
 - No one can read what you sent
 - No one can change what you sent
2. **Knowing who** you are communicating with
 - You are talking to who you think you are talking to and not someone else

Bob can't tell who the message is from



Bob can't tell who the message is from

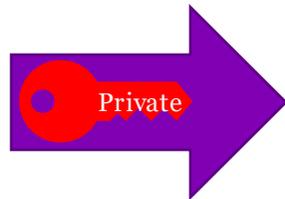
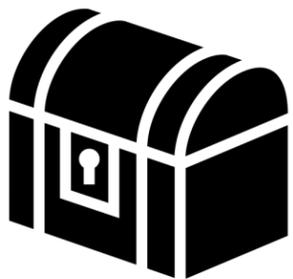


My public key

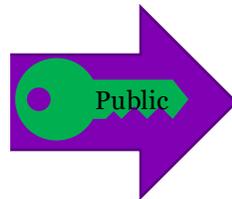


I want to prove a message is from me

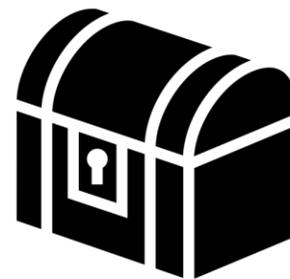
- I encrypt (lock) the message with my private key
- Anyone with the public key can use it to decrypt (unlock) the file. If it decrypts (unlocks), then it must have been encrypted (locked) by my private key and no other.



My private key



My public key



-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: GnuPG v2

```
mQENBFHMCGABCAC9WrYDO6K2L3VHy14eHN6suHLqMpJ+SO+IUTuLEVNuzLoXAUXH
KozHejfv/9XoG8j933ZtszXKCog3aMESeoEoz6fNGfolvaCe5B4jwqoJt8NHwb5L
B2dnqoCplgXcN2GJxfEHUaf27COSobCJxPMeshU4ZHke+g6DatmiEtBpVp41Ot
1zgxDMQkgb2H2xw28RYfykdDoueteIkOrFlrCy9ZF9KdMhA1eBH94KnwI QshdiZR
QYEX25+M8cKCb++Rc9H6an7EG9WHOFrW40UsY52OfveOyfQPzkkRto7u12339hvHo
B/h+7xLM6FQbOUZQ9BD5w7IQHgYtXJVsUjodABEBAAgOIkthbWkgVmFuaVWHIDxr
dmFuaWVhQGLuzi5jZC5hYy51az6JAT8EEwELACkFAIYKYvECCGyMFCQlMAYAHcwkI
BwMCAQYVCAIJcgsEFgIDAQIeAQIXgAAKCRCTdSxl9/HZffG+ CACShuKxje3QAqew
GWh8K4gCdiYoxDqJwq3PHxmyhZmQeN/1a1KcOrIj12b+Q75/5t+ EgXOHpRoP IxfG
LZ6zOEpf6A18fXx3JgQZdwPD0jtBiWNpOyMeBGTgIvEYg3so2VueQoeXcq3dbYp
5vstVxtD+TKHQ5CioIT75P2bzYq/XLT5aIbNqHQPcToYDgbRH+FvqsRXr7yeaef
JaPnxXo+1L33t2QY9zctiGyebwrVHMriPBj2VYCDzQk7JuQ5eFh4ZhsMgOmzLQD4
YiGr5weIMFwAvxZOARxAgVf48jiWvrXuJ8YfHWSohESeNOCYc2P8q2oLJwwE26T
lpdtrwCqtB1LYW1pIFZhbmlYSA8a2FtaUB2YW5pZWEuY29tPokBQgQTAQIALAIb
IwUJCWYBGAclCQgHAWIBBHULAgkKCwQWAqMBAh4BAheABQJWCmMeAhkBAaOJEJN2
zGX38dl9JJAIAIWoRxlYsrmKS6CbW8MgTxxTDOXA Ct1b7FoWoQZHskIUQhEcE+a
XBiyi1A5uHaatLfyjeXaD3qMEoZnQHoYMGEoGku00wWsbhfoQzHPgwzRLkDii75M
B1bawwoKWoV9e4AkMakXJcNf5BXe06AHRL2v15V205DikVnlCRXocKtu8b7LnmK
eLn7oLobr1deIuyKoNzbSnO/vpKDjpo/EY5yUeV9oIypZy/6wFQBehg1sXye6znO
9wb9uUs9+/P8pz4JILMDSevjfT7zSRSl/YP3fOfZ6N4bc+K0dwPM7u5Iyoeu0z
pzbv3ge7VhH2xIWz8yZv/2xT1345tWRRMOJAhweEwECAAyFALTnSpEACgkQjyxM
p99tBt2B8A/+OpIzOsQbQJB8yxti4I7PpD1weJdf3a81Vhm7JyXE/Xy66ypfdt3w
XmFRUulrwezY1NebWNCrQHqzQvRv/VJwjbTUx+Q3HsjIkKlhbE7iCiQXXtTRkoEny
2nuDcJGI2vo3C3B2JCucEw6esF1x79PI/IpV2+6tgUBKMDfOpsB2vbtqrHnmAYKL
4lQBfH1YSJgnzwo2JkhhocHdF9oZem1eMeiDeeVkh63893N8Swk5fBKdTj+SKZ/L
rQElBBlpMR9BmeY6bPvWRuyevKonIMR8oG9iFABxjTpWBL8aGk6EeVK5EqYDgVkd
ZlarK84r+KU1KD5IfgOCN7nhwgy7VI me68caZHSRiPWZP1fVVMhydiRjv8WsoUs6
InFVU3nxH+ZythPbYot86leGSchBT5K/fBQvbjhrRTbTFwvjzSifb9efWylDi994
nzP6cN0rir3GIpsT8gPGBB2/NjxaWiM6y3X1az1vRnsunQHuyKkFWPzwEvDJYaC
NN/3jWcbhLFwKBdsAhpS2+1meFPooJFvNetz2bjT9a9pXaQ6KhOm5DnhLcaV97
bFBpsUuBGaYZTSSo5x1RdXhqpEbgap8dtuHhVvJw9QYDQBjroK4aKyG9qqMD8cta
Pl/FAdyAqwH8Nw9efqAK+RQxSVUae9BYEnbIRpsDK6Mkp3YMFmu5ki5AQoEUcxy
AAEIALyXYy8G2ZaTdjPdGeRhmIqOOSUlzPV7/5E5BbYKBNu4KU3nX+JLvcF5jxPQ
42c7i/WRVxE1BJTiarKGSvC94TTXSIUKAt3T1oGBtXmGvqBGBq8jSGl1UTwdf
5yu5oJYRSf2fQRND6P/2eHNXejDUtdvhUXIU8h9MuUO/IpDoDnIwMnAATJHA+R
Zqw6oNpyjRGzvr3iUWuW4PtyJDI3ELAFkpb/NAc5TIuVHRHNOwNpldJhM5zHuB
QQb3G/EsCn2PQZ5w5SDzavF2SpvQfDqxYpDaTLAXiF+wsJL5iaUjxwRgJPoDbCZf
2Tozd7h9MXtGJdIPKJ8eLG8ogcMAEQEAAYkBJQYQAQIADwUcUcxyAAiBDAUJCWYB
gAAKCRCTdSxl9/HZfs+hB/9BJqSmIgcoHFxn1PVIKxekzL8+VWvM5Pk/EgMQSLZ2
HX4p3ial5PEPcYgUw9YnaG4ioodwJGw5/daTWRTzcnKd8YqoP+DU0t96HZDSu3m
mCzE9NVAQYboFvBmGoxo0627UBSvFqaXvABDYkoR8BoTnKhrQfWqXkZVb3ohKwD
TgAFjOGIziE6uAdST231tFaqobizYfe5AVXRqro2oxBqNbaJNqs3SWoD831Syvdv
lloBx83/Rogg7hUkI6F2vzXicWmUwFSXRggCSbLosHsP6isBWwvIHeRmna/aQab
YK3g3bV9jyczAS31gbogVLAZqNSWhp8vVIEE28Fyf/Ed
```

=x5FK

-----END PGP PUBLIC KEY BLOCK-----

My public key



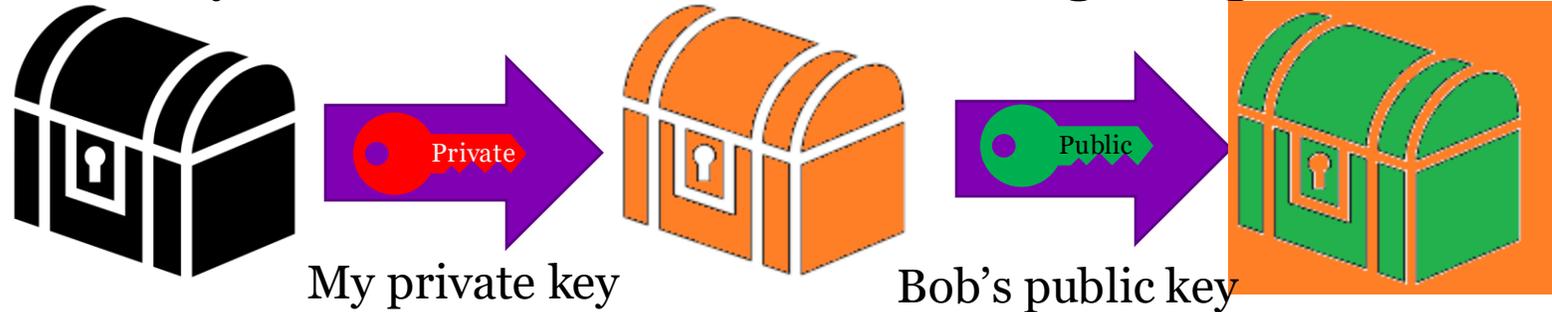
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

```
mQENBFHMCGABCAC9WfYDO6K2L3VHy14eHN6suHLqMpJ+SO+IUTuLEVnUzIoXAUXH
KozHejfv/9XoG8j933ZtszXKCog3aMESeoEoz6fNGfolvaCe5B4jwqoJt8NHwb5L
B2dnqoCplgXcN2GJxFeHHUaf27COsObCjXpMESHU4ZHke+g6DatmiEtBpVp41Ot
1zxdmQkqgb2H2xw28RYfykdOuetelkOrFLrCy9ZF9KdMhA1eBH94KnwI QshdiZR
QYEX25+M8cKCb++Rc9H6an7EG9WHOFrW40UsY52OfveOyfQPzkkRto7u12339hvHo
B/h+7xLM6FQbOUZQ9BD5w7IQHgYtXJVsUjodABEBAAgOIkthbWkgVmFuaWVhIDxr
dmFuaWVhQGluzi5jZC5hYy51az6JAT8EEwELACkFAlYKYvECCGyMFCQlMAYAHcWkI
BwMCAQYVCAIJCgsEFgIDAQIeAQIXgAAKCRCTdsxl9/HZffG+CACShuKxje3QAqew
GWh8K4gCdiYoxDqJwq3PHxmyhZmQeN/1a1KcOrIj12b+Q75/5t+EgXOHpRoP1xfG
LZ6zOEpf6A18IFXx3JgQZdwPD0jtBiWNPoyMeBGTgIvEYg3so2VueQoeXcq3dbYp
5vstvtD+TKHQ5CioIT75P2bzYq/XLT5aIbNqHQPcToO DgbRH+FvqsRXr7yeaef
JaPnxXo+1L33t2QY9zctiGyebwrvHMripBJ2VYCDzQk7J7uQ5eFh4ZhsMgOmzLQD4
YiGr5weIMFwAvxZOArXxAgVf48jiWvrXuJ8YfHWSohESeNOCYc2P8q2oLwwE26T
lpdtrwCqtB1LYW1pIFZhbmlYSA8a2FtaUB2YW5pZWEuY29tPokBQgQTAQIALAIb
IwUJCWYBgAcLQCgHAWIBBHUIAgkKCwQWAqMBAh4BAheABQJWCmMeAhkBAaOJEJN2
zGX38dl9JJAIAIwOrxrlYsrnKS6CbW8MgTxxTDOXA Ct1b7FoWoQZHskIUQhEcE+a
XBYibiA5uHaatLfyeXaD3qMEoZnQHoYMGEoGKUo0wWsbhfoQzHPgwzRLkDii75M
B1baWwoKWVb9e4AkMakXJcNf5BXeo6AHL2v15V205DikVnlCRXocKtu8b7LnmK
eLn7oLobr1deIuyKoNzbSnO/vpKDjPo/EY5yUeV9oIypZy/6wFQBehg1sXye6znO
9wb9uUs9+/P8pz4JILMDSevjfT7zSRSL/YP3fOfZ6N4bc+K0dwpM7u5Iyoeu9zh
pzibv3ge7VhH2xIWz8vYZ/2xT1345tWRRMOJAhweECAAyFALTnSpEACgkQjyxM
p99tBt2B8A/+OpIzOsQbQJB8yxti4I7PpD1weJDF3a81Vhm7JyXE/Xy66ypfdt3w
XmFRUulrwezYiNebWNCrQHHzQvRv/VJwjbTUX+Q3HsjIKlHbE7iCiQXtTRkoEny
2nu dcjGI2vo3C3B2JCucEw6esF1x79PI/Pv2+6tgUBKmDfOpsB2vbtqrHnmAYKL
4lQBfH1YSJgnzwo2JkhhcHdF9oZem1eMeiDeeVkh63893N8Swk5fBKdTj+SKZ/L
rQElBBlpMR9BmeY6bPvWRuyvKkonIMR8oG9iFABxjTpWBL8aGk6EeVK5EqYDgVkd
ZlarK84r+KU1KD5lfgOCN7nhwgy7VI me68caZHSRiPWZP1fVVMhydiRjv8WsoUs6
InFVU3nxH+ZythPbYoT86leGSchBT5k/fBQvbjhrRTbTfwvjzSifb9efWylDi994
nzP6cN0rir3GIpsT8gPGBB2/NjxaWiM6y3X1az1vRnsunQHuyKkFWPZwnEvDJYaC
NN/3jWcbhLFwKBDSaHps2+1meFPooJFvNetz2bjT9a9pDAQ6KJroK04aKyG9qqMD8cta
Pl/FAdyAqwH8Nw9efqAK+RQxSVUae9BYEnbIRpsDK6MkP3YMFmu5ki5AQoEUcxy
AAEIALyXYy8G2ZaTDJpdGcRhmIqOOSUlzPV7/5E5BbYKBNu4KU3nX+JLvcF5jxPQ
42c7i/WRVxE1BJTiarKGsEvCi94TTXSIUKAt3T1oGBtXmGvqbGBq8ljSGl1UTwdf
5yu5oJyRSf2fQRND6P/2eHNXejDUtdvhUXIU8h9MuUO/ipDoDnIvMnAATJHA+R
Zqw6oNpyjRGzvr3juWUwe4PtyJDI3ELAFkbp/NAc5TIuVHRHNOwnpldJhM5zHuB
QQb3G/EsCn2PQZ5w5SDzavF2SpvQfDqxYpDaTLAXtF+wsJL5iaUjxwRgJPoDbCZf
2Tozd7h9MXtGJDIPKJ8eLG8ogcMAEQEAAYkBJQYQAIA DWUCUcxyAAIbDAUJCWYB
GAAKCRCTdsxl9/HZfS+hB/9BJqSmIgcoHFxnbiPVIKxekzL8+VWm5Pk/EgMQSLZ2
HX4p3ial5PEPEYgUw9YnaG4ioodwJGw5/dATWRRtZcnKd8YqoP+DUOT96HZDSu3m
mCzE9NVAQYboFvBmGOXoe627UBSvFqaXvABDYkoR8BoTnKhrQfWqXkZVb3ohKwD
TgAFjOGIZiE6uAdST231tFaqobizYfe5AVXRqro2oxBqNbaJNqs3SWoD83iSyvdv
lloBx83/Rogg7hUkI6F2vzXicWmUwFSXRrggCSbLosHsP6isBWwvIHeRmna/aQab
YKG3gbV9jyczAS31gbogVLAZqNSWhp8vVIEE28Fyf/Ed
=x5FK
```

-----END PGP PUBLIC KEY BLOCK-----

If I do both of those at the same time I can prove that:

1. only I could have sent the message (signature)



My private key

Bob's public key

2. only Bob can read it (encryption)



My public key

Bob's private key

Encryption properties we want:

1. The communication between you and the other party is **confidential** and has **not been changed**
 - No one can read what you sent
 - No one can change what you sent
2. **Knowing who** you are communicating with
 - You are talking to who you think you are talking to and not someone else

LINKING KEYS AND IDENTITIES

But we still have a problem:

All that assumes that we know which key goes with which person.

One of the founding problems in Usable Security and Privacy.

Even now we have no good answer.

How do we solve the identity problem?

Idea: Have the humans do the linking of identity to cryptographic keys.

We could post the public key somewhere highly public and verifiable it came from us.

PSIRT PGP Key (0x33E9E596) X

Secure | https://blogs.adobe.com/psirt/?page_id=146

blogs.adobe.com Search Blogs

Adobe Product Security Incident Response Team (PSIRT) Blog

Working to help protect customers from vulnerabilities in Adobe software. Contact us at [PSIRT\(at\)adobe\(dot\)com](mailto:PSIRT(at)adobe(dot)com).

PSIRT PGP Key (0x33E9E596)

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: Mailvelope v1.8.0
Comment: https://www.mailvelope.com

xsFNBfM/2KMBEADbwToJM3BCVE1OeC22HgVEqNEDppXzuD2dgfKuy0M4tx2L
De7GkPjo6AOsw4yi8bakLiidpw5B0J/AR1VtIjIDeMs0F9MRZicV0UKyA5qV
c9BafZnAicY7nezkIJUmyLcIVMC60pqSHzo0Ewy2PZjxzcI4vDGHmcgfV5X
R+duYld3LtVI+A/5jv326LB16bcNts/tOhW2T0LraMPOctdH84Z4tPcyp335
s8/dZ2C+eOMD4iX1kIymZ1kqEfZNVcs1sRUXy27sL01VHCYmi6UNWCeeHOu2
2yJxMiBCniozBKZUwCR6ysg97nng633dN9mf7V30PS3zAjhe0Hvmzg3B/Nfo
qzy2dAEU/JDUBhiAo+xr9VF3ZPOoC8JySORgyUm/2t3TTBaH+DnfsUBiqo5U
2T0n8x2R1FWxyZYNCTku5JOvPqRBft13DSyJD7LDDps62nqhpavb34eprwuk
qIk0TMRu9mB4EQc+cNFR3ZpN1AKj+HOb/TUJwCJpVju2/3g0wgdqHh+OQ1vC
Nm8vIGnQZwQ30WqnH/UFoh3RPJ+WqnDq88NmQBq8I4aNV4u8MgoObd/zrtVX
kAwYHbIZLo925NjFyPuuxhWiCotKen18dZefB8aB81RjyUMnCJ0GQus+JG8
TJyEesNdK/q8HD5h1kCRSzMHD1+Ra3z/1+FFIwARAQABzR1BZG9iZSBQU01S
VCA8cHNpcnRAYWRvYmUuY29tPslBewQQAQgALwUCWb/YrWUJAEZgAYLCQgH
AwIJEIbAD8Kvh3YWBbUIAgoDFgIBAhkBAhsDAh4BAADk2A//f+6PFzg4VmLI
PzstZPoqPR/1X1Z7RIYbQosHvsFwyW0WwX1uIlsEeD5Qo7HQ6NNMAOW51Js
wFvFOWIa9U6SHRoU1kGTSESReOq5HnXe4DcBubsKmoMS68PuiZ88wYOIM4Up
9V9PUuaue0U4oSrYHnH5qBOqurtv8wO5Cq4uTwnfnjN7n4OH0++2910PJ68B
6+kMuQyG4swmxsZh1j1qGMHcs0c/BuI3W+n5w+xLM7N5jjCTjNXR+tGmstdm
RPEoLW0so+ZFwfNW0CLKjYUahp3p6H9x8R13wrp2re0GhQKRgt3D4UcAgsPs
```

CATEGORIES

- Alert
- Security Bulletins and Advisories
- Uncategorized

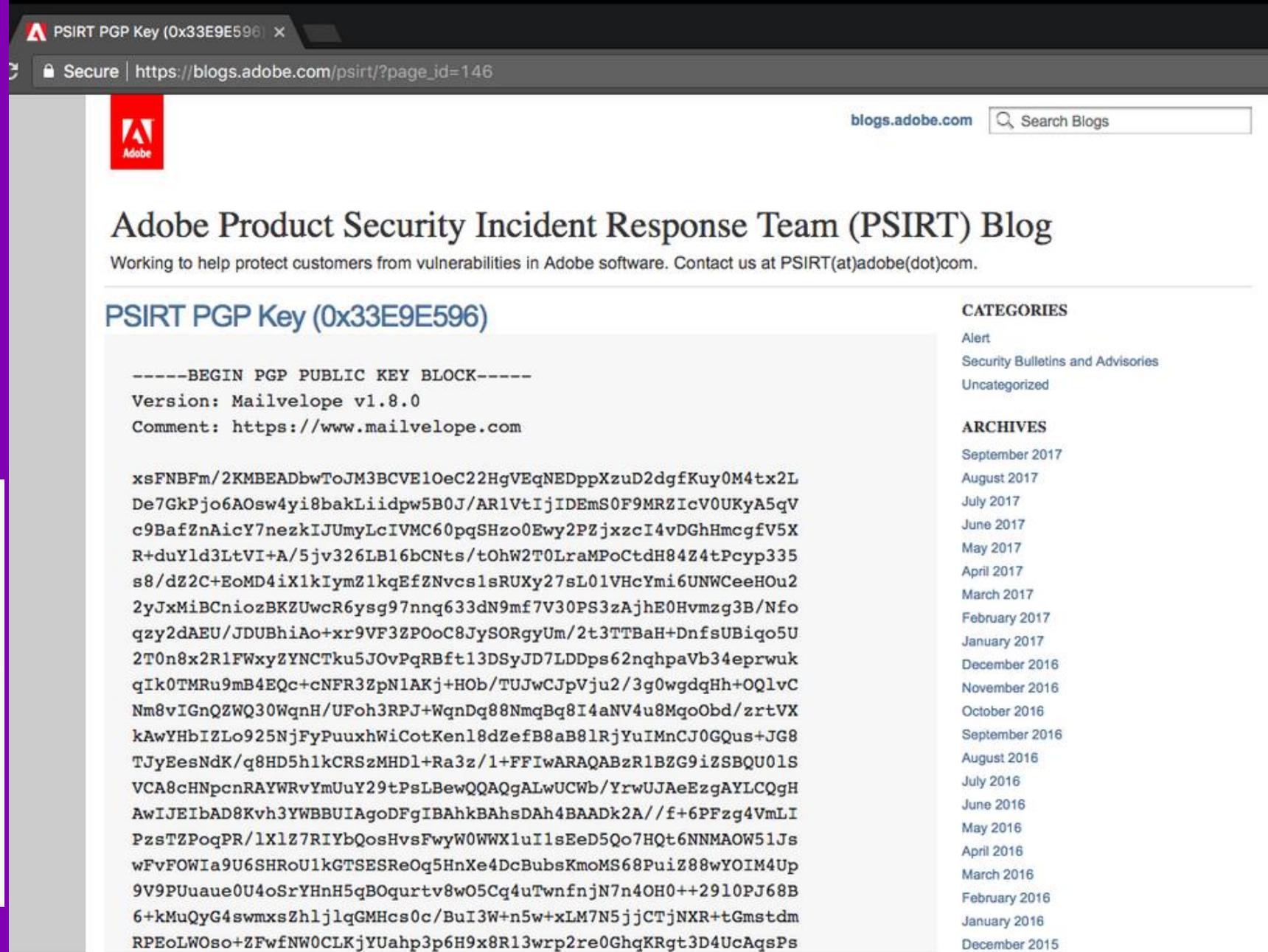
ARCHIVES

- September 2017
- August 2017
- July 2017
- June 2017
- May 2017
- April 2017
- March 2017
- February 2017
- January 2017
- December 2016
- November 2016
- October 2016
- September 2016
- August 2016
- July 2016
- June 2016
- May 2016
- April 2016
- March 2016
- February 2016
- January 2016
- December 2015

Photo credit: Juho Nurminen @jupenur

Other people can then compare the keys on their computers to the highly visible copy.

```
xsFNBFm/2KMBEADbwToJM3BCVE1OeC22HgVEqNEDppXzuD2dgfKuy0M4tx2L
De7GkPjo6AOsw4yi8bakLiidpw5B0J/AR1VtIjIDeMS0F9MRZicV0UKyA5qV
c9BafZnAicY7nezkJIjUmYlCIVMC60pqSHzo0Ewy2PZjxzcI4vDGhHmcgfV5X
R+duYld3LvtVI+A/5jv326LB16bcNts/tOhW2T0LraMPoCtdH84Z4tPcyp335
s8/dZ2C+eOMD4iX1kIymZ1kqEfZNVcs1sRUXy27sL01VHCYmi6UNWCeeHOu2
2yJxMiBCniozBKZUwcr6ysg97nnq633dN9mf7V30PS3zAjhE0Hvmzg3B/Nfo
qzy2dAEU/JDUBhiAo+xr9VF3ZPOoC8JySORgyUm/2t3TTBaH+DnfsUBiqo5U
2T0n8x2R1FWxyZYNCTku5JOvPqRBft13DSyJD7LDDps62nqhpaVb34eprwuk
qIk0TMRu9mB4EQc+cNFR3ZpN1AKj+HOb/TUJwCJpVju2/3g0wgdqHh+OQ1vC
Nm8vIGnQZwQ30WqnH/UFoh3RPJ+WqnDq88NmQBq8I4aNV4u8MgoObd/zrtVX
kAwYHbIZLo925NjFyPuuxhWiCotKen18dZefB8aB81RjYUImnCJ0GQus+JG8
TJyEesNdK/q8HD5h1kCRSzMHD1+Ra3z/1+FFIwARAQABzR1BZG9iZSBQU01S
VCA8cHNpcnRAYWRvYmUuY29tPslBewQQAQgALwUCWb/YrWUJAeEzGAYLQgH
AwIJEIbAD8Kvh3YWBUIAgoDFgIBAhkBAhsDAh4BAADk2A//f+6PFzg4VmLI
PzsTZPoqPR/lXlZ7RIYbQosHvsFwyW0WwX1uIlsEeD5Qo7HQ6NNMAOW51Js
wFvFOWIa9U6SHRoU1kGTSESReOq5HnXe4DcBubsKmoMS68PuiZ88wYOIM4Up
9V9PUuaue0U4oSrYHnH5qBOqurtv8wO5Cq4uTwnfnjN7n4OH0++2910PJ68B
6+kMuQyG4swmxsZhlj1qGMHcs0c/BuI3W+n5w+xLM7N5jjCTjNXR+tGmstdm
RPEoLW0so+ZFwfNW0CLKjYUahp3p6H9x8R13wrp2re0GhqKRGt3D4UcAqsPs
```



The screenshot shows a web browser window with the address bar displaying "Secure | https://blogs.adobe.com/psirt/?page_id=146". The page header includes the Adobe logo and the text "blogs.adobe.com" with a search bar. The main heading is "Adobe Product Security Incident Response Team (PSIRT) Blog" with a sub-heading "Working to help protect customers from vulnerabilities in Adobe software. Contact us at PSIRT(at)adobe(dot)com." The article title is "PSIRT PGP Key (0x33E9E596)". The content of the post is a PGP public key block, starting with "-----BEGIN PGP PUBLIC KEY BLOCK-----" and ending with "-----". The key block includes the version "Mailvelope v1.8.0" and a comment "https://www.mailvelope.com". The key data is a long alphanumeric string. On the right side of the page, there are sections for "CATEGORIES" (Alert, Security Bulletins and Advisories, Uncategorized) and "ARCHIVES" (listing months from September 2017 to December 2015).

Photo credit: Juho Nurminen @jupenur

Though we must be careful to post ONLY the public key...

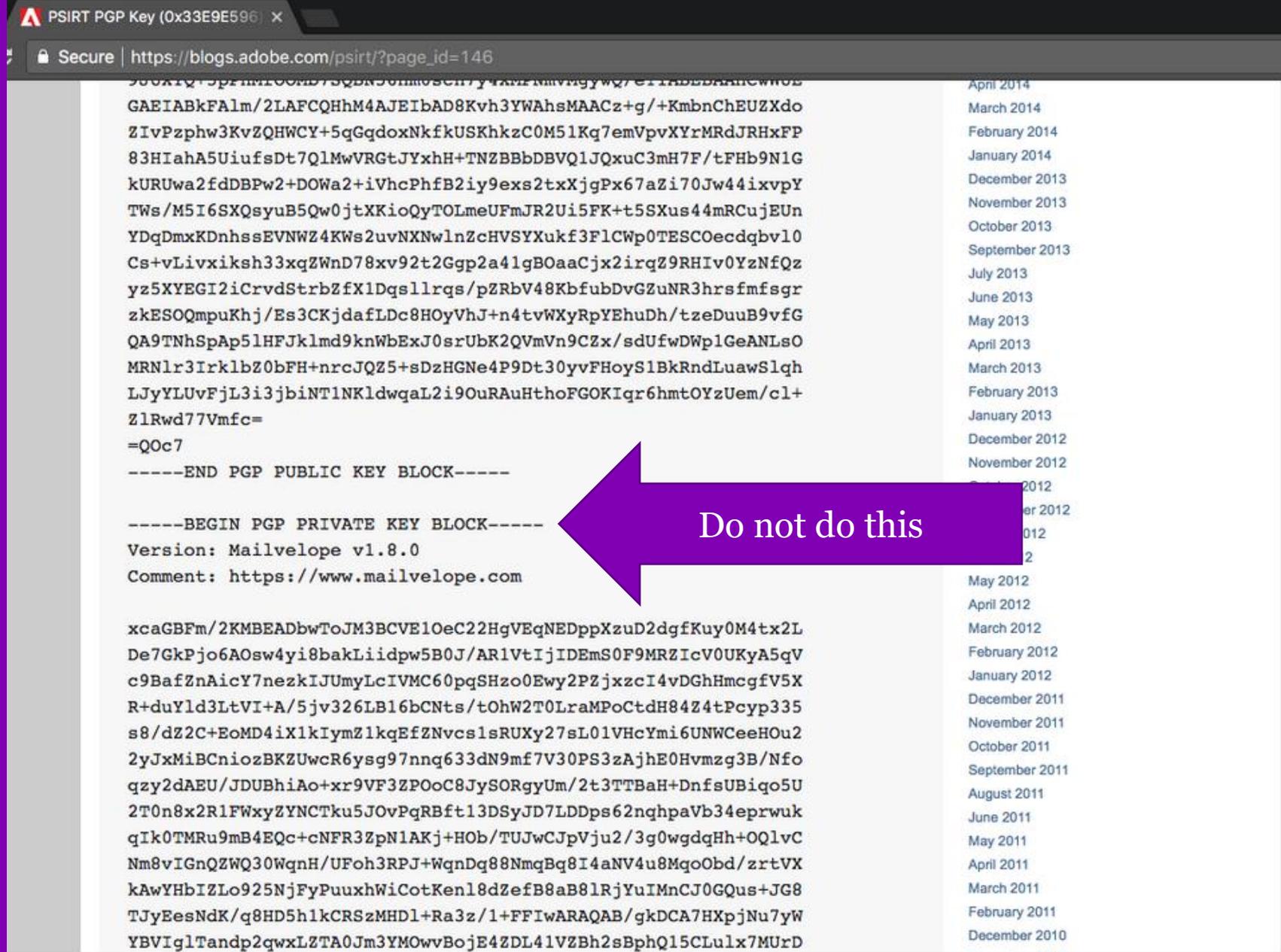


Photo credit: Juho Nurminen @jupenur

Nice idea, but it does not scale.

Also a chicken-and-egg problem. How do we find a place guaranteed to be from us without using cryptography?

Idea 2: What if everyone did a few verifications. We could slowly build a web of verifications like:

Alice verified Bob's key

Bob verified Charlie's key

so

Alice can trust Charlie's key

Web of trust

- Alice hand verifies that Bob's public key really does belong to Bob
- Then Alice "signs" the key by encrypting it with her private key.
- Now anyone that has hand verified Alice's key, can also trust Bob's key (if they trust Alice to do verifications).

My public key

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

```
mQENBFHMcgABCAC9WrYDO6K2L3VHy14eHN6suHLqMpJ+SO+IUTuLEVNuzIoXAUXH
KozHejV/9XoG8j933ZtszXKCog3aMESeoEoz6fNGfolvaCe5B4jwqoJt8NHwb5L
B2dnqoCplgXcN2GJxfEHHUaf27COsObCjXpMESHU4ZHke+g6DatmiEtBpVp41Ot
1zgdMqKgb2H2xw28RyfykdDoueteIkOrFlrCy9ZF9KdMhA1eBH94KnwI QshdiZR
QYEX25+M8cKCb++Rc9H6an7EG9WHOFrW40UsY52OfveOyfQPzkkRto7u12339hvHo
B/h+7xLM6FQbOUZQ9BD5w7IQHyYtXJVsUjodABEBAAgOIkthbWkgVmFuaVWvHIDxr
dmFuaWVhQGluZi5lZC5hYy51az6JAT8EEwELACKfAlYKYvECCGyMFCQlMAYAHcwkI
BwMCAQYVCAIJcgsEFgIDAQIEAQIXgAAKCRCTdsxl9/HZffG+ CACShuKxje3QAqew
GWh8K4gCdiYoxDqJwq3PHxmyhZmQeN/1a1KcOrIj12b+Q75/5t+EgXOHpRoP IxfG
LZ6zOEpf6A18iFxx3JgQZdwPD0jtBiWNpOyMeBGTgIvEYg3so2VueQoeXcq3dbYp
5vstVxtD+TKHQ5CioIT75P2bzYq/XLT5aIbNqHQPcTooDgbRH+FvqsRXr7yeaef
JaPnxXo+1L33t2QY9zctiGyebwrvHMriPBj2VYCDzQk7JuQ5eFh4ZhsMgOmzLQD4
YiGr5weIMFwAvxZOaRxEagVf48jiWvrXuJ8YfHWSohESeNOCYC2P8q2olwwE26T
lpdtrwCqtB1LYW1pIFZhbmllySA8a2FtaUB2YW5pZWEuY29tPokBQgQTAQIALAIB
IwUJCWYBgaAcLCQgHAwIBBhULAgkKCwQWAqMBAh4BAheABQJWCmMeAhkBAaOJEJN2
zGX38dl9JJAIAIWorxIYsrmKS6CbW8MgTxxTDOXA Ct1b7FoWoQZHskIUQhEcE+a
XYyib1A5uHaatLfyjeXaD3qMEoZnQHoYMGEoGku00wWsbhfoQzHPgwzRLkDii75M
BibaWwoKWoVB9e4AkMakXJcNf5BXe06AHL2v15V205DikVnlCRXocKtu8b7LnmK
eLn7oLobr1deIuyKoNzbSnO/vpKDjpo/EY5yUeV9oIypZy/6wFQBehg1sXye6znO
9wb9uUsu9+/P8pz4JILMDSevjfT7zSRSl/YP3fOfZ6N4bc+K0dwpM7u5Iyoeuqzh
pzibv3ge7VhH2xIWz8vYZ/2xT1345tWRRMOJAhwEEwECAAyFALTnSpEACgkQjyxM
p99tBt2B8A/+OpIzOsQbQJB8yxti4I7PpD1weJdf3a81Vhm7JyXE/Xy66ypfdt3w
XmFRUulrwezYiNebWNCrQHzQvRv/VJwjbTUx+Q3HsjkKlHbE7iCiQXxtTRkoEny
2nuDcGI2vo3C3B2JCucEw6esF1x79PI/IPv2+6tgUBKmDfOpsB2vbtqrHnmAYKL
4lQBFH1YSJgnzwo2JkhhcHdF9oZem1eMeiDeeVkh63893N8Swk5fBKdTj+SKZ/L
rQElBBlpMR9BmeY6bPvWRuyevKonIMR8oG9iFABxjTpWBL8aGk6EeVK5EqYDgVkd
ZlarK84r+KU1KD5lfgOCN7nhwgy7VI me68caZHSRiPWZP1fVVMhydiRjv8WsoUs6
InfVU3nxH+ZythPbYot86leGSchBT5K/fBQvbjhrRTbTFwvjzSifb9efWylDi994
nzP6cNOrir3GIpsT8gPgbB2/NjxaWiM6y3X1az1vRnsunQHuyKkFWPZwnEvDJYaC
NN/3jWcbhLFwKBdsAhpS2+1meFpooJFvNetz2bjT9a9pXaQ6KhOmo5DnhLcaV97
bFBpsUuBGaYZTSSo5x1RdXhqpEbgap8dtuHhVvJw9QYDQBjroK4aKyG9qqMD8cta
Pl/FAdyAqwH8Nw9efqAK+RQxSVUae9BYEnbIRpsDK6MkP3YMFmu5ki5AQoEUcxy
AAEIALyXYy8G2aTDJpdGcRhmIqOOSUlzPV7/5E5BbYKBNu4KU3nX+JLvcF5jxPQ
42c7i/WRVxE1BJTiarKGSvEvCig94TTXSIUKAt3T1oGBtXmGvqbGBq8ljSGl1UTwdf
5yu5oJyRSf2fQRND6P/2eHNXejDUtdvhUXIU8th9MuUO/ipDoDnwIvMnAATJHA+R
Zqw6oNpyjRGzvr3i uWUwe4PtyJDI3ELAFkbp/NAc5TIuVHRHNOwnpldJhM5zHuB
QQb3G/EsCn2PQZ5w5SDzavF2SpvQfDqxYpDaTLAXtF+wsJL5iaUjxwRgJPodbCZf
2Tozd7h9MXtGJDlPKJ8eLG8ogcMAEQEAAYkBJQYQAQIADwUcUcxyAAIBDAUJCWYB
gAAKCRCTdsxl9/HZfS+hB/9BJqSmIgcOHFXnb1PVIKxekzL8+WVm5Pk/EgMQSLZ2
HX4p3ial5PEPcYgUw9YnaG4ioodwJGw5/daTWrrTzcnKd8YqoP+DUOt96HZDSu3m
mCzE9NVAQYboFbVmGOxoeo627UBSvFqaXvAxBDYkoR8BoTnKhrQFwXkZVb3ohKwD
TgAFjOGLZiE6uAdST231tFaqobizYfe5AVXRqro2oxBqNbaJNqs3SWoD83iSyvdv
lIOBx83/Rogg7hUkI6F2vzXicWmUwFSXRrggCSbLosHsP6isBWwvIHeRmna/aQab
YKG3gbV9iyzAS31gbogVLAZqNSWhp8vVIEE28Fyf/Ed
=x5FK
-----END PGP PUBLIC KEY BLOCK-----
```

Wonderful idea in theory. But verifying those long keys is hard... also I don't trust most people to do a thorough job of it.....

Idea 3: What if a couple of trusted groups did the verifications. Then they could have high standards and everyone could just trust them.

Certificate Authorities

- A certificate authority verifies some properties of a person/organization and issues a “certificate” signed by their private key.
- Certificates can be quite detailed about what has been verified, and what they have been verified to do.

Certificate Hierarchy

▾ QuoVadis Root CA 2

▾ QuoVadis EV SSL ICA G1

www.ease.ed.ac.uk

Certificate Fields

Issuer

▾ Validity

Not Before

Not After

Subject

▾ Subject Public Key Info

Subject Public Key Algorithm

Subject's Public Key

Field Value

Modulus (2048 bits):

```
9d 6b 8a 90 ff 2a c7 ad 11 f0 5f 95 ff 34 f5 c1
fa 9b d6 38 9c d6 90 49 8f b5 2c 9c 8b 51 ec 74
9b 69 17 ed b7 25 8c c0 8c ac 90 28 55 97 00 0b
d2 e4 88 c5 4b 03 ae 3d 73 d6 92 ac 25 06 99 39
b1 13 c8 2a 56 9d 6d 89 47 b0 eb 8b e8 c8 17 25
fd 60 1c b6 f5 62 fb 5f 82 33 cb a5 5d 0f 24 92
25 04 c2 16 4a 35 66 a6 66 b3 c5 75 ff 5e cb 94
31 c6 e6 a5 aa f4 3a 40 72 42 e4 93 43 b2 a6 0e
```

Export...

Certificate Authorities are used by browsers to verify identity

Online Banking, CDs, Mo x +

Ally Financial Inc. (US) https://www.a Search

Ally Financial Inc.
Secure Connection

You are securely connected to this site,
owned by:

Ally Financial Inc.
Detroit
Michigan, US

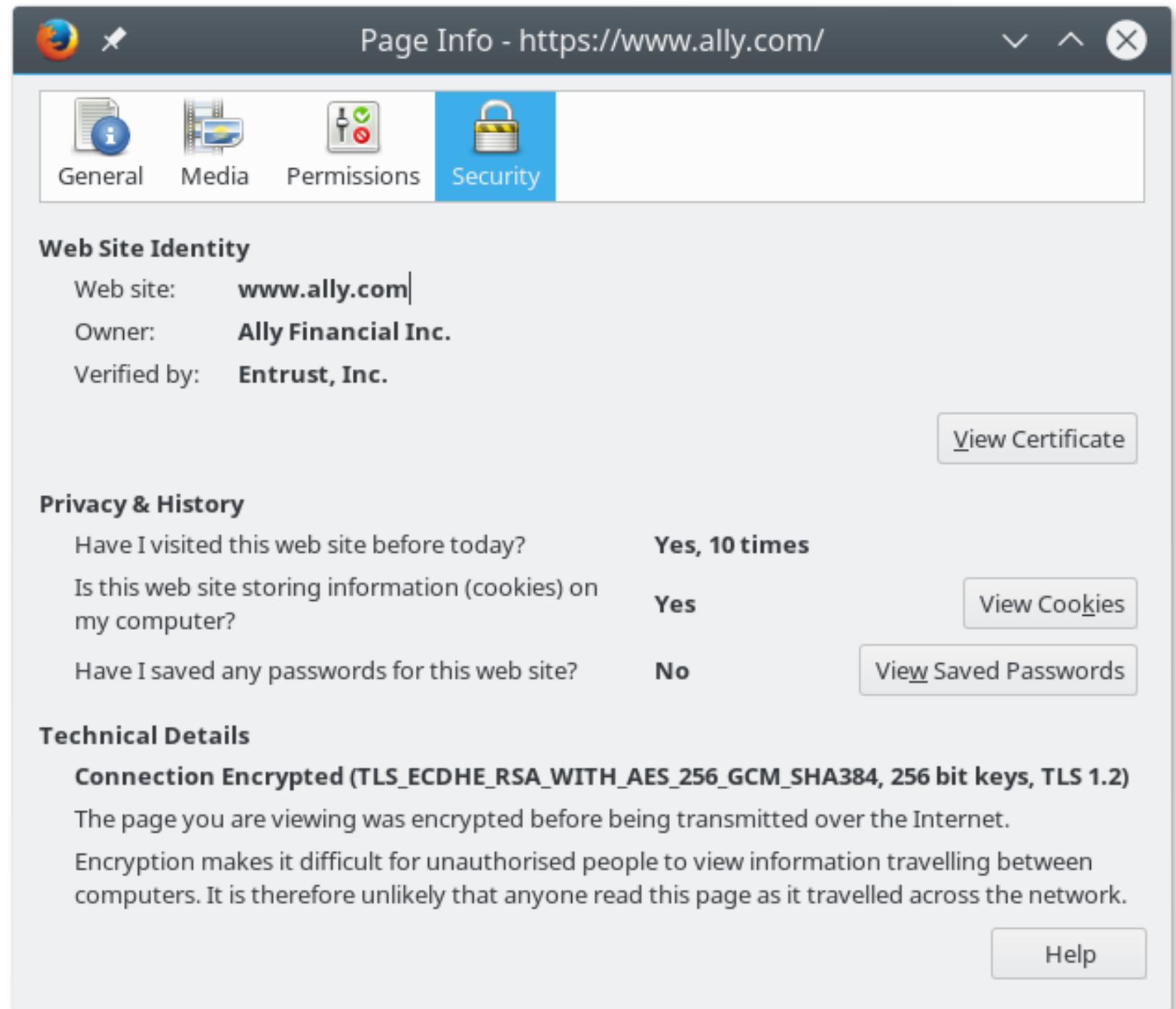
Verified by: Entrust, Inc.

More Information

Whether it's banking, credit card,
home loans or auto finance, nothing stops
us from doing right by you.

View Ally Bank Auto Online Banking on the Why Choose Ally

You can see lots of details about any encrypted connection.



The screenshot shows a browser's 'Page Info' window for the URL <https://www.ally.com/>. The window has a dark header with the title 'Page Info - https://www.ally.com/' and navigation icons. Below the header is a tabbed interface with four tabs: 'General', 'Media', 'Permissions', and 'Security'. The 'Security' tab is selected and highlighted in blue. Under the 'Security' tab, there are three sections: 'Web Site Identity', 'Privacy & History', and 'Technical Details'. The 'Web Site Identity' section lists: Web site: **www.ally.com**, Owner: **Ally Financial Inc.**, and Verified by: **Entrust, Inc.**. To the right of this section is a button labeled 'View Certificate'. The 'Privacy & History' section contains three rows of information: 'Have I visited this web site before today?' with the answer 'Yes, 10 times'; 'Is this web site storing information (cookies) on my computer?' with the answer 'Yes' and a 'View Cookies' button; and 'Have I saved any passwords for this web site?' with the answer 'No' and a 'View Saved Passwords' button. The 'Technical Details' section is titled 'Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, 256 bit keys, TLS 1.2)' and contains two paragraphs explaining that the page is encrypted and that encryption makes it difficult for unauthorized people to view information traveling between computers. At the bottom right of the window is a 'Help' button.

Page Info - <https://www.ally.com/>

General Media Permissions **Security**

Web Site Identity

Web site: **www.ally.com**
Owner: **Ally Financial Inc.**
Verified by: **Entrust, Inc.**

[View Certificate](#)

Privacy & History

Have I visited this web site before today?	Yes, 10 times	
Is this web site storing information (cookies) on my computer?	Yes	View Cookies
Have I saved any passwords for this web site?	No	View Saved Passwords

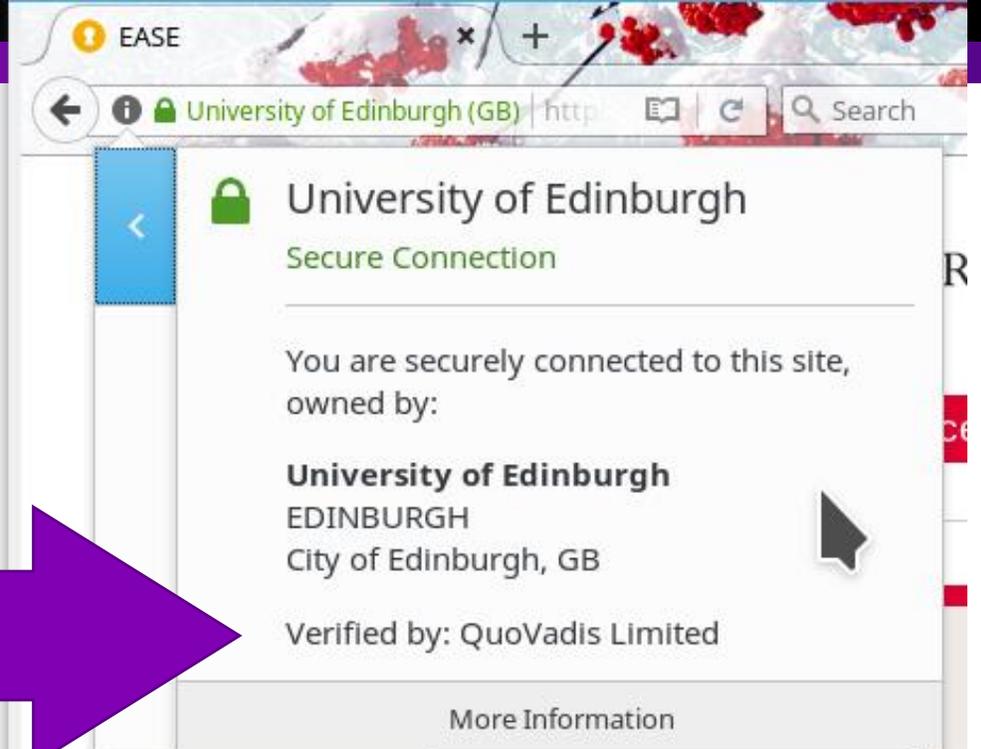
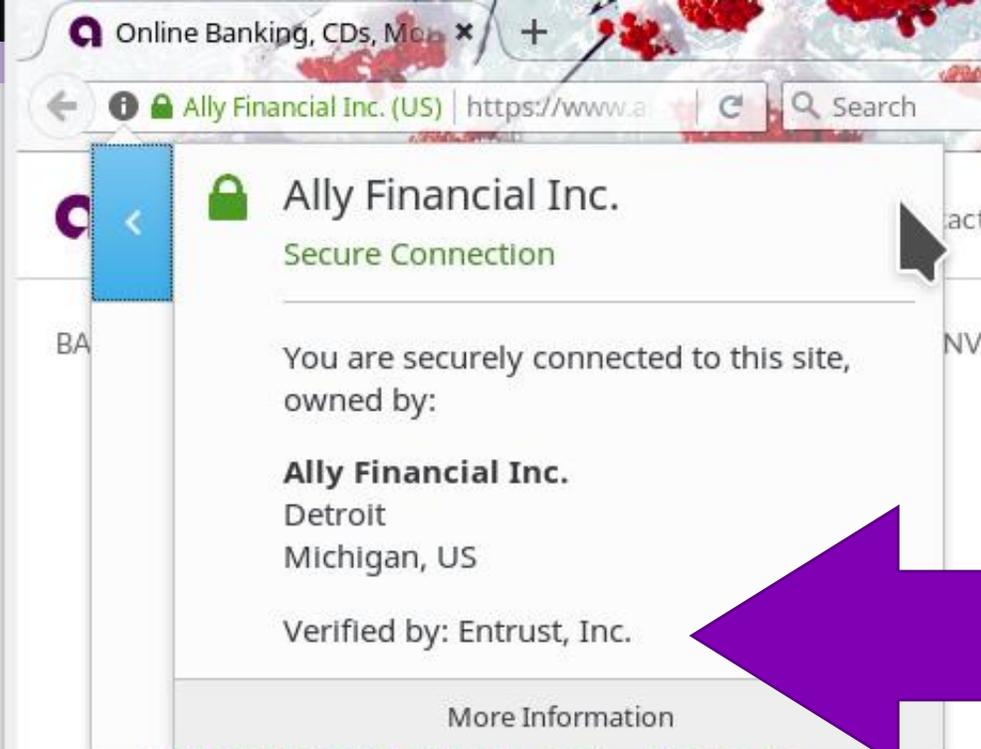
Technical Details

Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, 256 bit keys, TLS 1.2)

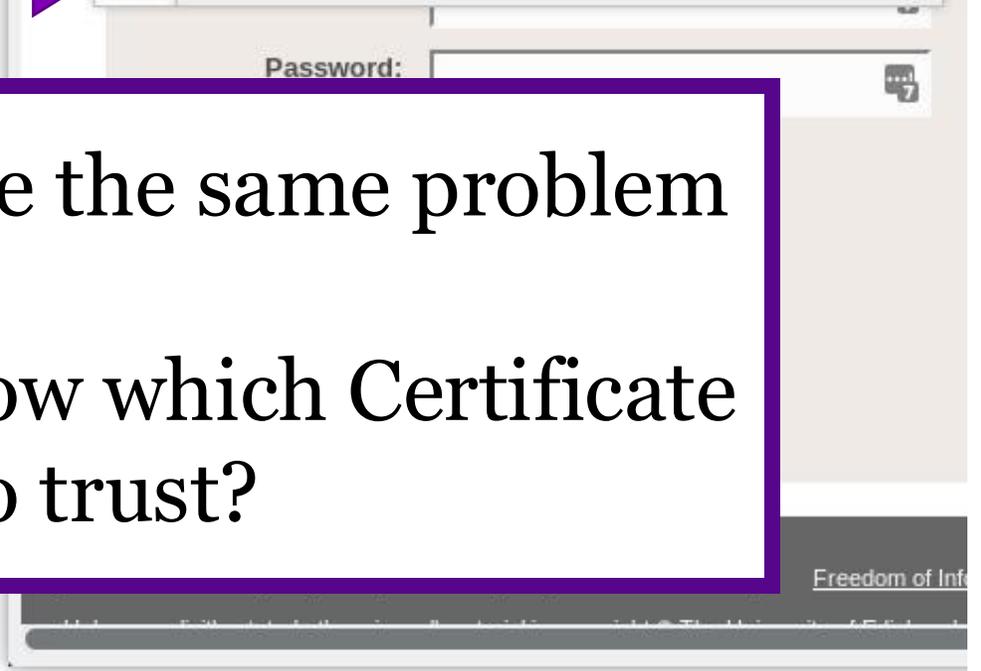
The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorised people to view information travelling between computers. It is therefore unlikely that anyone read this page as it travelled across the network.

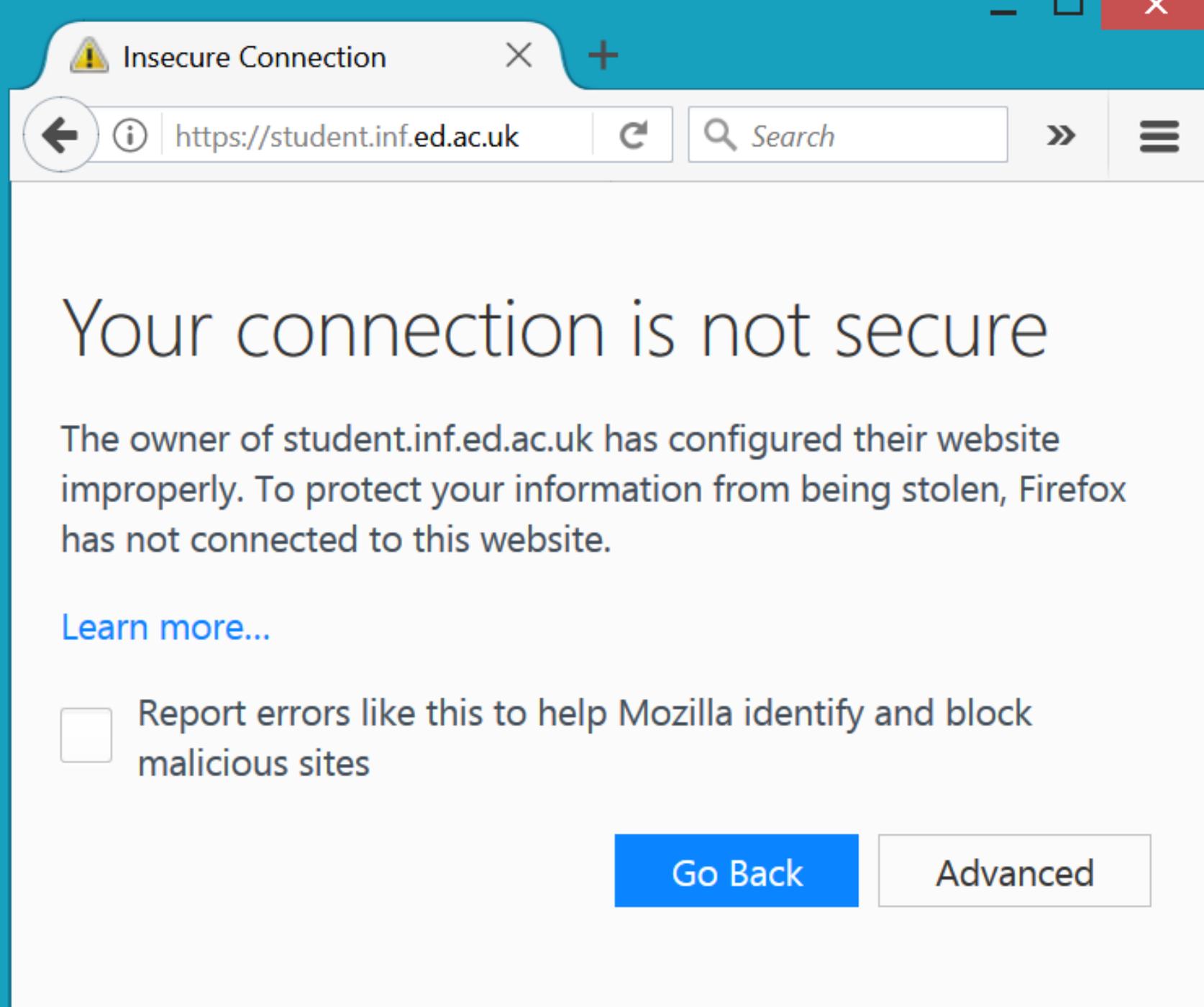
[Help](#)



But now don't we just have the same problem again?
How does the browser know which Certificate Authorities to trust?



**Clearly some
Certificate
Authorities are
trusted and some
are not.**



The image shows a Firefox browser window with a teal title bar. The address bar displays a warning icon (a yellow triangle with an exclamation mark) and the text "Insecure Connection". The address bar also shows the URL "https://student.inf.ed.ac.uk" and a search box with the placeholder text "Search". The main content area of the browser displays a large heading "Your connection is not secure" in a dark blue font. Below the heading, there is a paragraph of text: "The owner of student.inf.ed.ac.uk has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website." Underneath this text is a link "Learn more..." in blue. At the bottom of the page, there is a checkbox that is currently unchecked, followed by the text "Report errors like this to help Mozilla identify and block malicious sites". At the bottom right, there are two buttons: a blue button labeled "Go Back" and a white button with a grey border labeled "Advanced".

Insecure Connection

<https://student.inf.ed.ac.uk> Search

Your connection is not secure

The owner of student.inf.ed.ac.uk has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

[Learn more...](#)

Report errors like this to help Mozilla identify and block malicious sites

[Go Back](#) [Advanced](#)

Your operating system and your browser both maintain lists of Certificate Authorities that they trust.

These lists differ between operating systems, browsers, and organizations.



INFOWORLD TECH WATCH

By [Fahmida Y. Rashid](#), Senior Writer, InfoWorld | MAR 24, 2017

About |

Informed news analysis every weekday

Google to Symantec: We don't trust you anymore

Admins need to consider whether they still want to use Symantec after its repeated mistakes with issuing TLS certificates



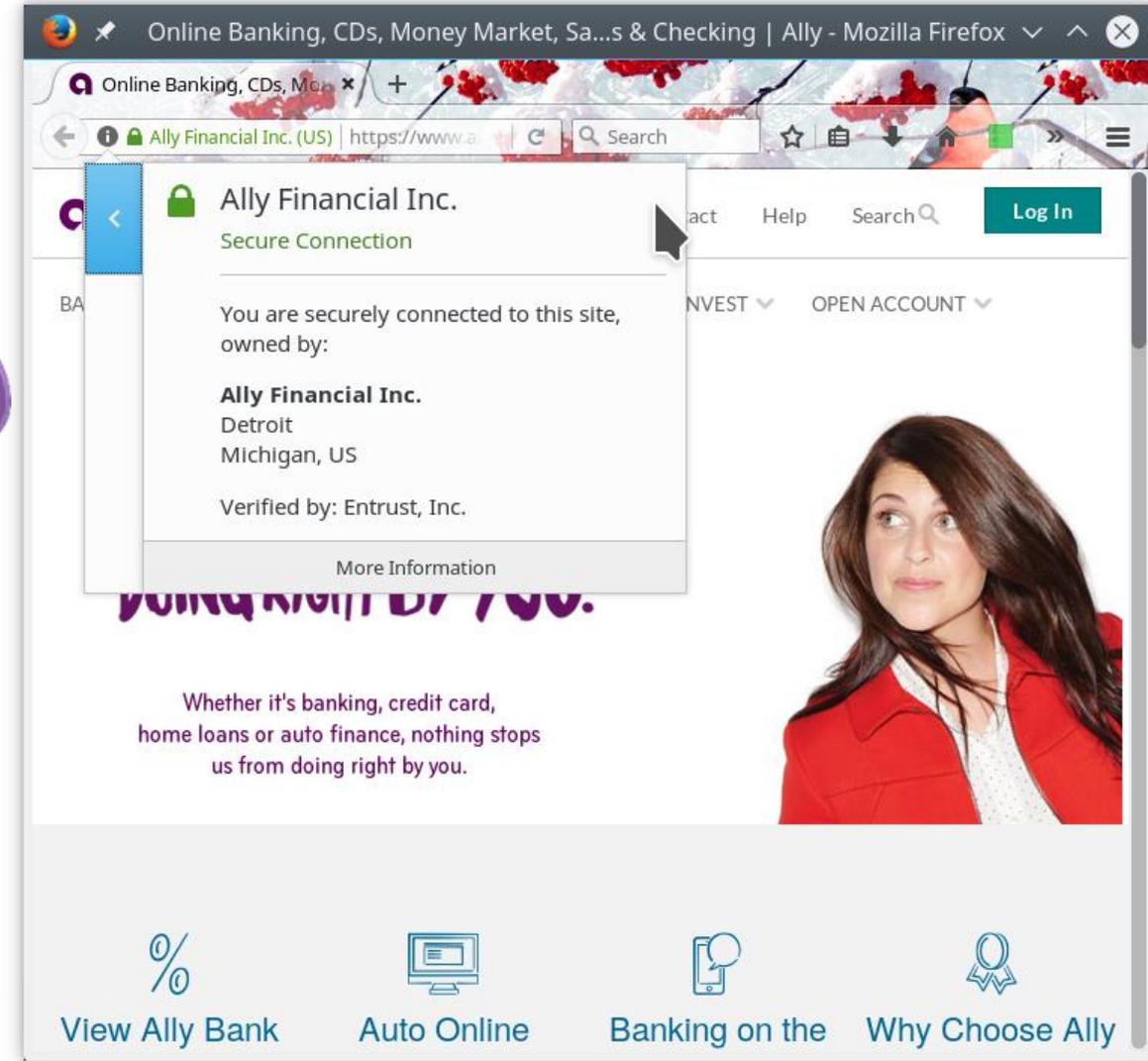
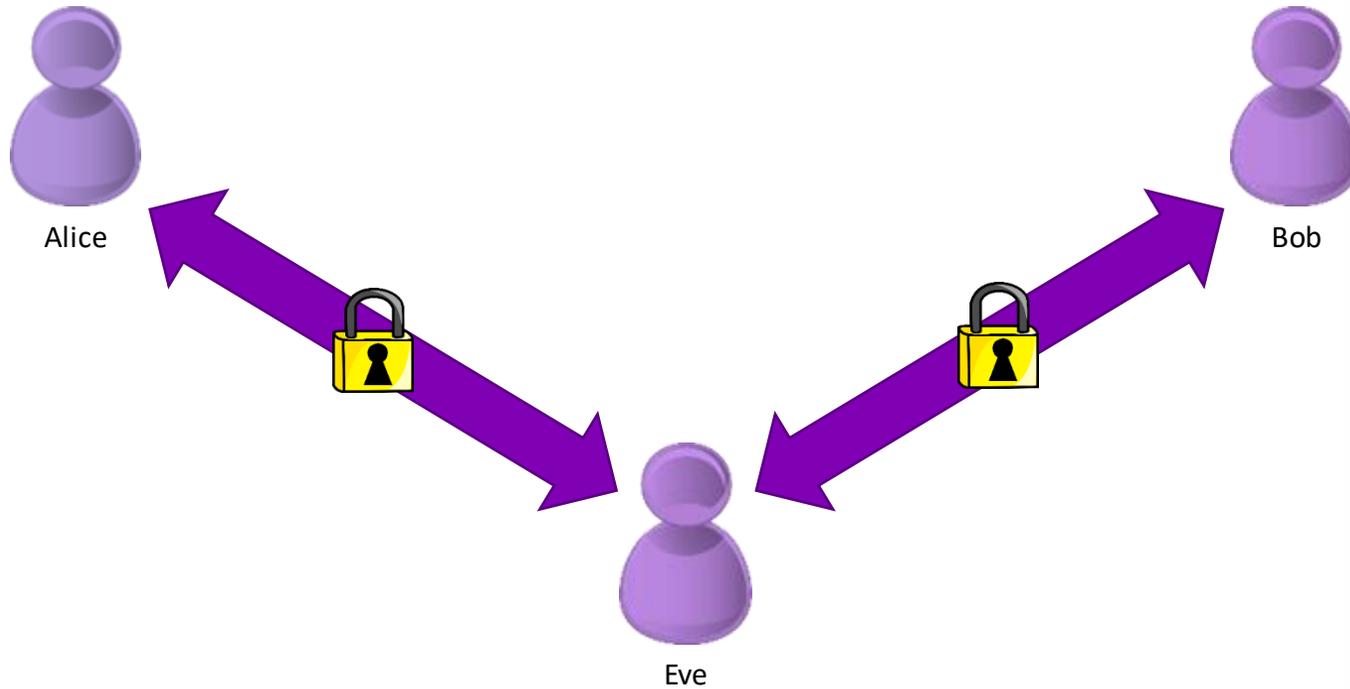
geralt via pixabay

Security teams, network administrators, and operations teams have busy days ahead. Google's Chrome development team is fed up with Symantec as a certificate authority and has announced plans to no longer trust current Symantec certificates.

In the past 18 months, Google has tangled repeatedly with Symantec over the way it issues transport layer security (TLS) certificates, with Symantec promising to do better. The latest incident—an investigation into 127 mis-issued certificates—ballooned into “at least 30,000, issued over a period spanning several years,” Ravi Sleevi, a software engineer on the Google

Each organization makes its own trust decisions about Certificate Authorities

In Conclusion...



Why Johnny Can't Encrypt

Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0

Alma Whitten
*School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213
alma@cs.cmu.edu*

J. D. Tygar¹
*EECS and SIMS
University of California
Berkeley, CA 94720
tygar@cs.berkeley.edu*

Abstract

User errors cause or contribute to most computer security failures, yet user interfaces for security still tend to be clumsy, confusing, or near-nonexistent. Is this simply due to a failure to apply standard user interface design techniques to security? We argue that, on the contrary, effective security requires a different usability standard, and that it will not be achieved through the user interface design techniques appropriate to other types of consumer software.

To test this hypothesis, we performed a case study of a security program which does have a good user interface by general standards: PGP 5.0. Our case study used a cognitive walkthrough analysis together with a laboratory user test to evaluate whether PGP 5.0 can be successfully used by cryptography novices to achieve effective electronic mail security. The analysis found a number of user interface design flaws that may

1 Introduction

Security mechanisms are only effective when used correctly. Strong cryptography, provably correct protocols, and bug-free code will not provide security if the people who use the software forget to click on the encrypt button when they need privacy, give up on a communication protocol because they are too confused about which cryptographic keys they need to use, or accidentally configure their access control mechanisms to make their private data world-readable. Problems such as these are already quite serious: at least one researcher [2] has claimed that configuration errors are the probable cause of more than 90% of all computer security failures. Since average citizens are now increasingly encouraged to make use of networked computers for private transactions, the need to make security manageable for even untrained users has become critical [4, 9].

Why
Enc

If an average user of email feels the need for privacy and authentication, and acquires PGP with that purpose in mind, will PGP's current design allow that person to realize what needs to be done, figure out how to do it, and avoid dangerous errors, without becoming so frustrated that he or she decides to give up on using PGP after all?

interface by general standards: PGP 5.0. Our case study used a cognitive walkthrough analysis together with a laboratory user test to evaluate whether PGP 5.0 can be successfully used by cryptography novices to achieve effective electronic mail security. The analysis found a number of user interface design flaws that may

the probable cause of more than 90% of all computer security failures. Since average citizens are now increasingly encouraged to make use of networked computers for private transactions, the need to make security manageable for even untrained users has become critical [4, 9].

ive when used
rovably correct
ovide security if
to click on the
y, give up on a
re too confused
need to use, or
rol mechanisms
able. Problems
s: at least one
ration errors are

Understanding the problem

Definition: Security software is usable if the people who are expected to use it:

1. are reliably made aware of the security tasks they need to perform;
2. are able to figure out how to successfully perform those tasks;
3. don't make dangerous errors; and
4. are sufficiently comfortable with the interface to continue using it.

Users need to:

- understand that privacy is achieved by encryption, and figure out how to encrypt email and how to decrypt email received from other people
- understand that authentication is achieved through digital signatures, and figure out how to sign email and how to verify signatures on email from other people
- understand that in order to sign email and allow other people to send them encrypted email a key pair must be generated, and figure out how to do so
- understand that in order to allow other people to verify their signature and to send them encrypted email, they must publish their public key, and figure out some way to do so
- understand that in order to verify signatures on email from other people and send encrypted email to other people, they must acquire those people's public keys
- manage to avoid such dangerous errors as accidentally failing to encrypt, trusting the wrong public keys, failing to back up their private keys, and forgetting their pass phrases
- be able to succeed at all of the above within a few hours of reasonably motivated effort

Tested usability using two methods

- Cognitive Walkthrough
 - A set of experts review the experts and make an informed guess about what will be problematic
 - Paired with heuristics – The experts state how the user interface supports or violates common HCI principles (Heuristics)
- Lab Study
 - Ask the participant to perform a set of tasks
 - Very similar to a think aloud, but without the talking aloud part

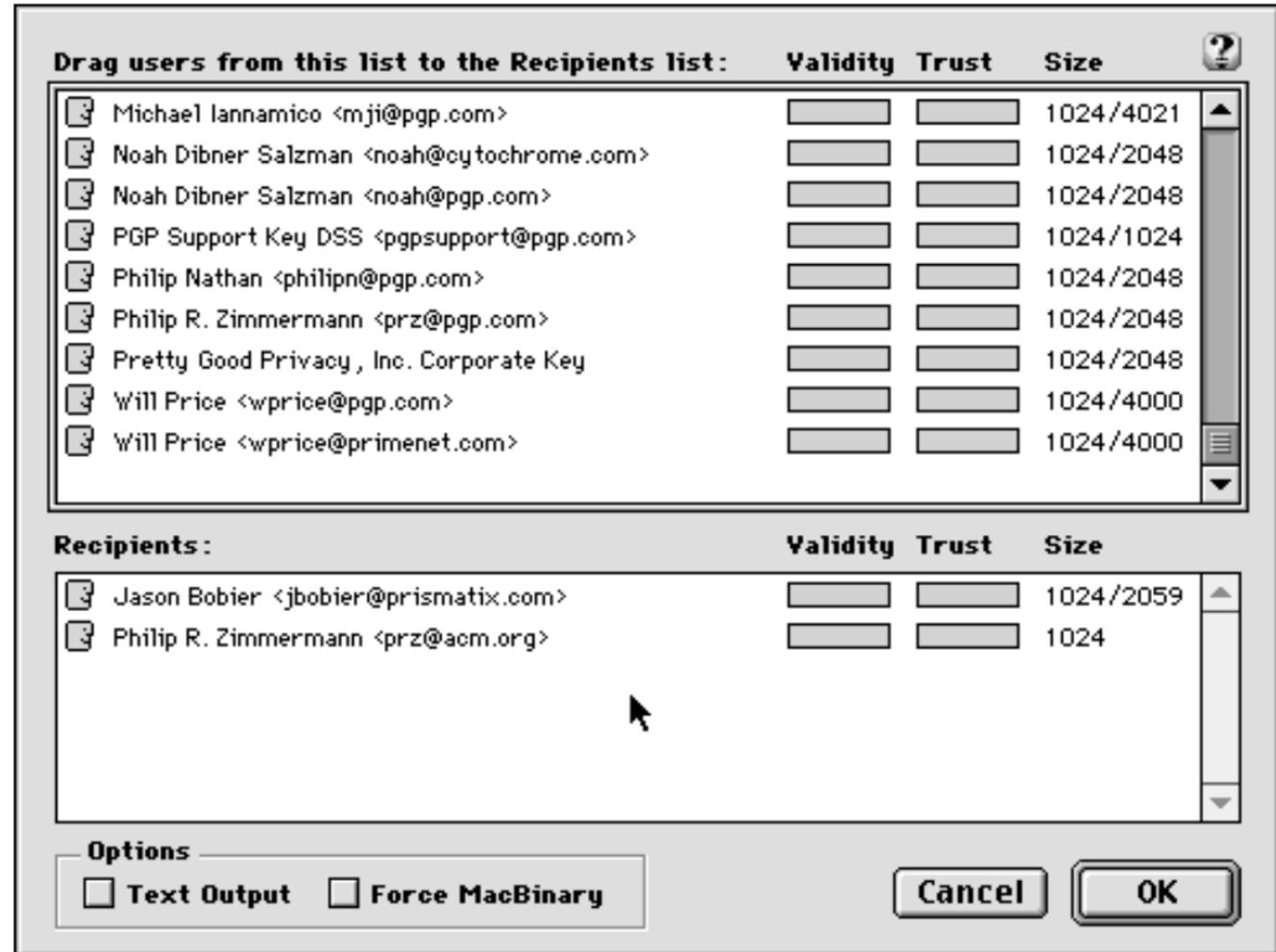
Cognitive walkthrough outcomes

- **Visual metaphors** – Do key and lock pictures make sense?
- **Different key types** – Public vs private keys, or maybe signing and encryption keys?
- **Key server** – Used for sharing keys
- **Key management policy** – Trust and validity ratings
- **Consistency** – Use of the same terms everywhere
- **Too much information** – Information like key size, hashes, and trust
- **Irreversible actions**
 - Accidentally deleting the private key
 - Accidentally publicizing a key
 - Accidentally revoking a key
 - Forgetting the pass phrase
 - Failing to back up the key rings

Lab study

- 12 participants with CS backgrounds
- Participant had to send several emails to team members (the researchers)
 - Creating a key pair
 - Sending their public key to team members
 - Getting team members' public keys
 - Sending the email
 - Decrypting response email
- 3 – emailed the private key to the team member
 - 1 never realized the error
- 1 – forgot their pass phase and had to re-generate keys
- 1 – never figured out how to encrypt
- 7 – used their public keys to encrypt
 - 1 created a separate key pair for each team member
- 3 – successfully sent an encrypted email to the whole team and were able to decrypt an response email

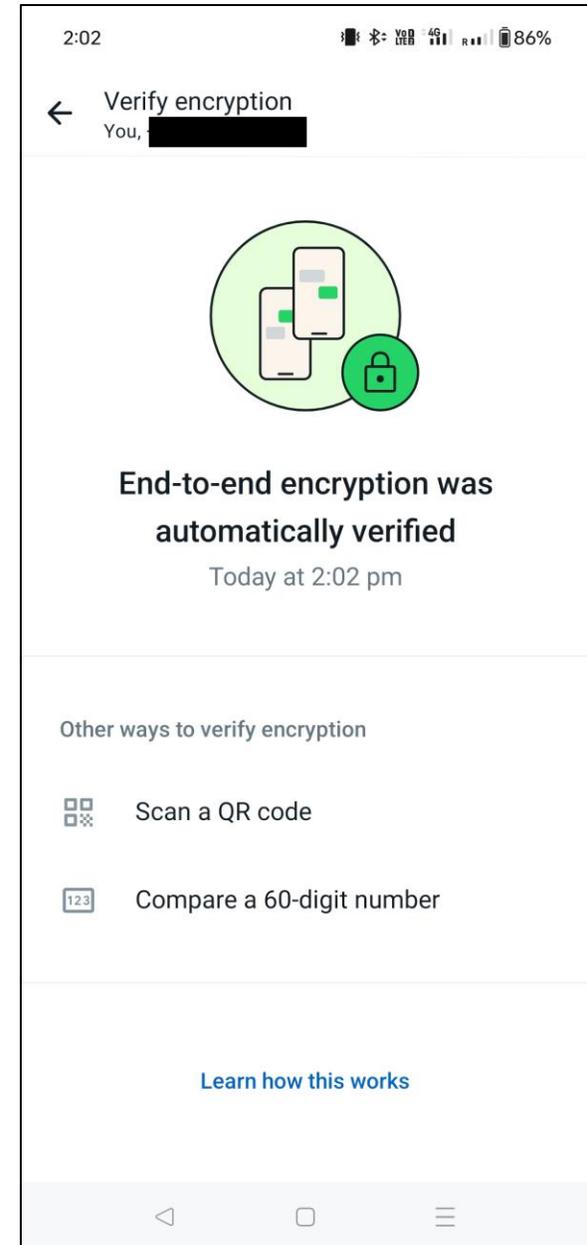
Whitten and Tygar evaluated PGP encryption in 1999, surely it must be more usable now.



"SECURE" MESSAGING

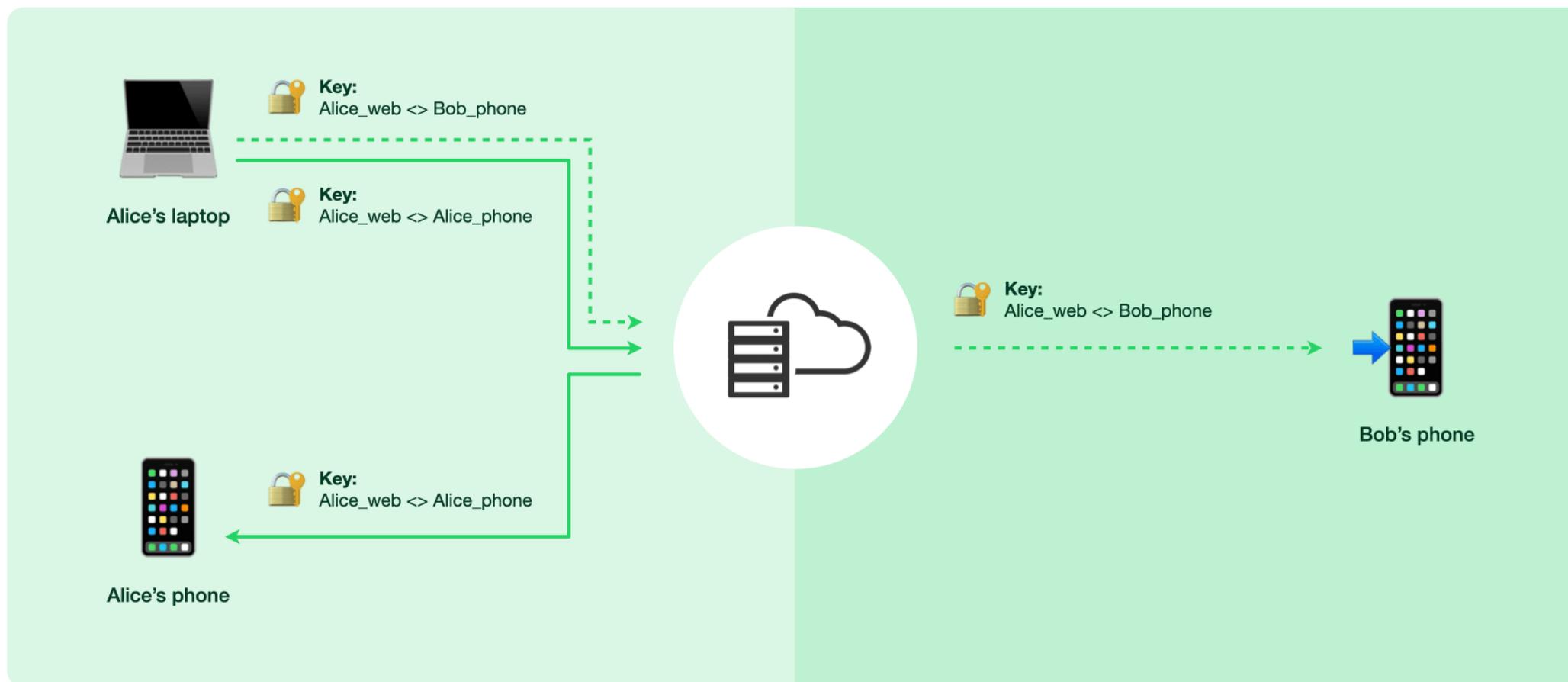
WhatsApp

- All messages, including group chats, are end-to-end encrypted
- The “ends” are the WhatsApp app on both devices
- Keys are managed by WhatsApp itself and shared with the devices as needed



WhatsApp: syncing chats

Life of a message: Multi-Device (new)

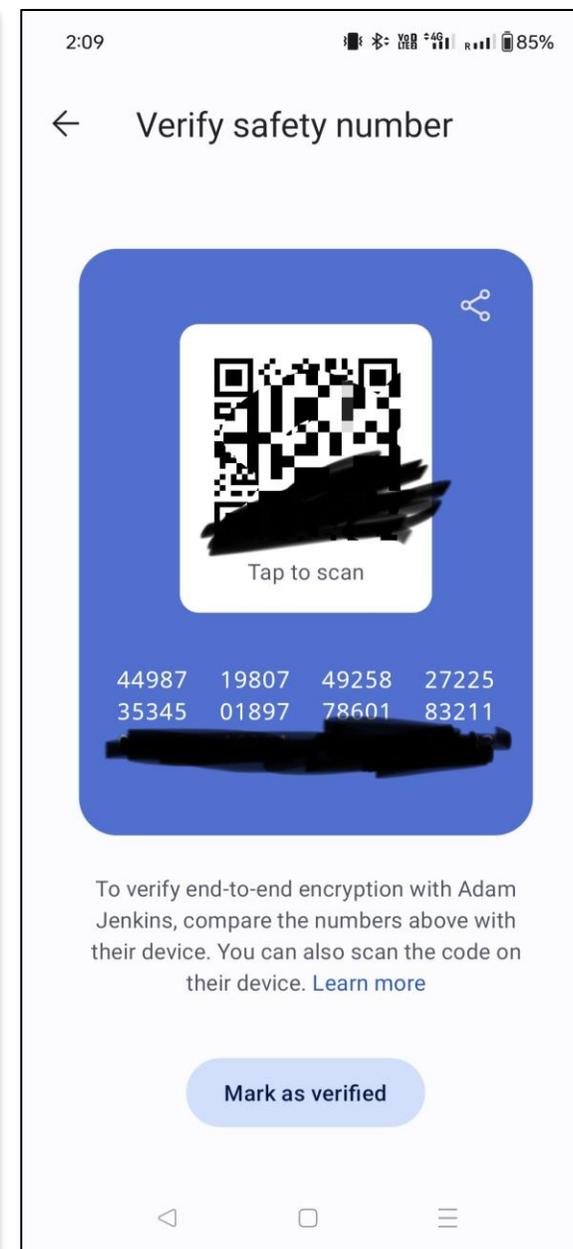
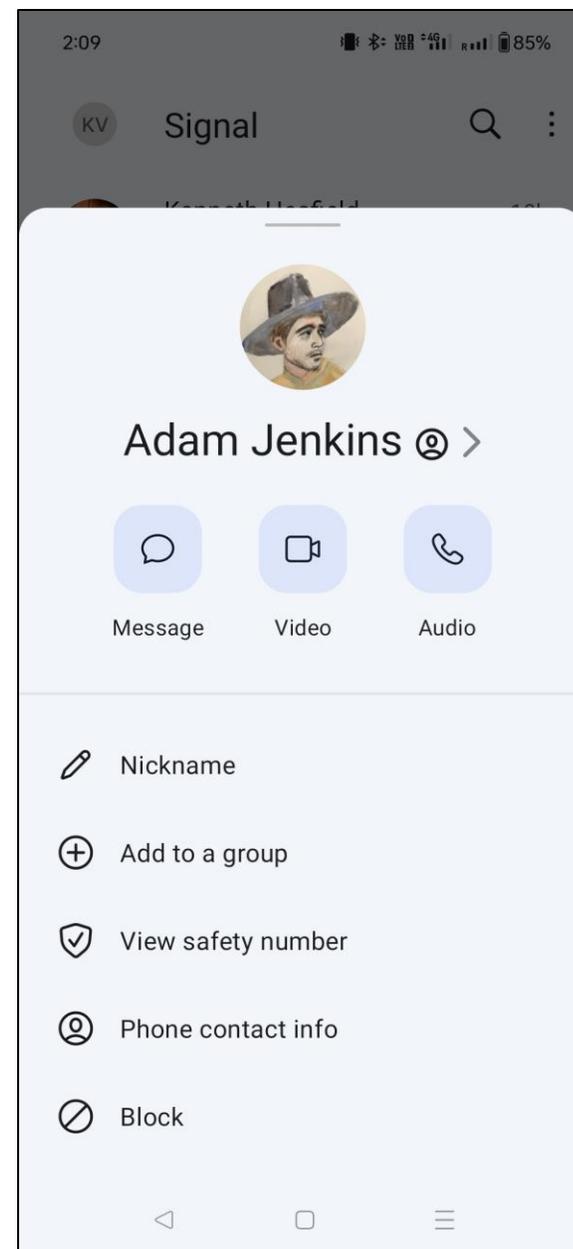


→ - - - → End-to-end encrypted channels

<https://engineering.fb.com/2021/07/14/security/whatsapp-multi-device/>

Signal

- End to end encrypted
- The “ends” are the apps on both sides



Telegram

- Only Secret chats are end-to-end encrypted
- Secret chats are more restricted than other messaging tools
- Video and audio calls are end-to-end encrypted

Why Telegram?



Simple

Telegram is so simple you already know how to use it.



Private

Telegram messages are heavily encrypted and can self-destruct.



Synced

Telegram lets you access your chats from multiple devices.



Fast

Telegram delivers messages faster than any other application.



Powerful

Telegram has no limits on the size of your media and chats.



Open

Telegram has an open API and source code free for everyone.



Secure

Telegram keeps your messages safe from hacker attacks.



Social

Telegram groups can hold up to 200,000 members.



Expressive

Telegram lets you completely customize your messenger.

The Security Blanket of the Chat World: An Analytic Evaluation and a User Study of Telegram

Ruba Abu-Salma^{1,*}, Kat Krol^{2,*†}, Simon Parkin¹, Victoria Koh¹, Kevin Kwan¹, Jazib Mahboob¹, Zahra Traboulsi¹, and M. Angela Sasse¹

¹ University College London (UCL), {ruba.abu-salma.13, s.parkin, victoria.koh.13, kevin.kwan.13, jazib.mahboob.13, zahra.traboulsi.13, a.sasse}@ucl.ac.uk

² University of Cambridge, kat.krol@cl.cam.ac.uk

Abstract—The computer security community has advocated widespread adoption of secure communication tools to protect personal privacy. Several popular communication tools have adopted end-to-end encryption (e.g., WhatsApp, iMessage), or promoted security features as selling points (e.g., Telegram, Signal). However, previous studies have shown that users may not understand the security features of the tools they are using, and may not be using them correctly. In this paper, we present a study of Telegram using two complementary methods: (1) a lab-based user study (11 novices and 11 Telegram users), and (2) a hybrid analytical approach combining cognitive walk-through and heuristic evaluation to analyse Telegram’s user interface. Participants who use Telegram feel secure because they feel they are using a secure tool, but in reality Telegram offers limited security benefits to most of its users. Most participants develop a habit of using the less secure default chat mode at all times. We also uncover several user interface design issues that impact security, including technical jargon, inconsistent use of terminology, and making some security features clear and others not. For instance, use of the end-to-end-encrypted *Secret Chat* mode requires both the sender and recipient be online at the same time, and *Secret Chat* does not support group conversations.

I. INTRODUCTION

Recent events have seen developers offering messaging tools with greater security to support a diverse range of user motivations. These include revelations about mass surveillance and the potential for user tracking in communication tools (e.g., Facebook’s tentative plans to use WhatsApp user data [30]). End-to-end (E2E) encryption has been adopted in several messaging tools (e.g., WhatsApp, iMessage), whereas other tools have positioned security as a key selling point

(e.g., Telegram, Signal). Security-related features may differ in how much they involve the user, whereas differences in the visibility of security features can create problems and impact user trust in a messaging tool [52], [53]. Telegram [1] is unique in offering separate modes of communication with differing levels of security. However, it may be difficult for users to distinguish between these modes and make effective use of them [31]. Users may explore the functionality of a messaging tool, or identify features that satisfy specific goals (which may or may not relate to security, such as sharing sensitive information with others). Users new to a security tool may also use it in ways that are not anticipated by developers [46].

Here, we explore the motivations and security behaviours of using a messaging tool that claims to be secure, specifically those who have not used Telegram before and those who are familiar with the tool. We combine two research techniques: (1) a novel lab-based user study with 11 novices and 11 participants with prior experience of using Telegram, and (2) a usability inspection bringing together cognitive walk-through and heuristic evaluation, focusing on Telegram’s UI. This approach has been applied before in the area of usable security, most notably by Whitten and Tygar [62] to evaluate PGP 5.0. Here, we have planned a lab-based study that uses a set of tasks to elicit user perceptions of Telegram. The usability inspection complements this by allowing us to look at issues not touched upon by those tasks or not reported by our participants.

Prior work has focused on novices, with the admirable goal of identifying barriers to adoption [52], [62]. Studies of secure communication tools have rarely involved non-novices, where these users can identify the motivations for adopting and using security features in practice. Participants brought their mobile devices to the lab. Novices installed Telegram to explore its features by way of a ‘sensitive payment information’ messaging scenario. Prior users of Telegram were similarly involved in the task, but as an opportunity to see how they have used the tool and the role of Telegram’s various security features in these practices, such as the *Secure Chat* mode. In both cases, scenario tasks were used to promote discussion as part of semi-structured interviews. Use of a System Usability Scale (SUS) questionnaire further explored the usability of the tool for novices and users alike. We found that both groups

When asked about encryption, six participants (three novices and three users) provided explanations relating to security and safety. These included “*an extra barrier of security*”, “*more time is needed to know the content of the message*”, and “*making chats safe from hacking until they get deleted from the servers.*”

*Authors contributed equally.

†The study was conducted while the author was at University College London (UCL).

Questions