

ECE458/ECE750T27: Computer Security

Cryptography

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



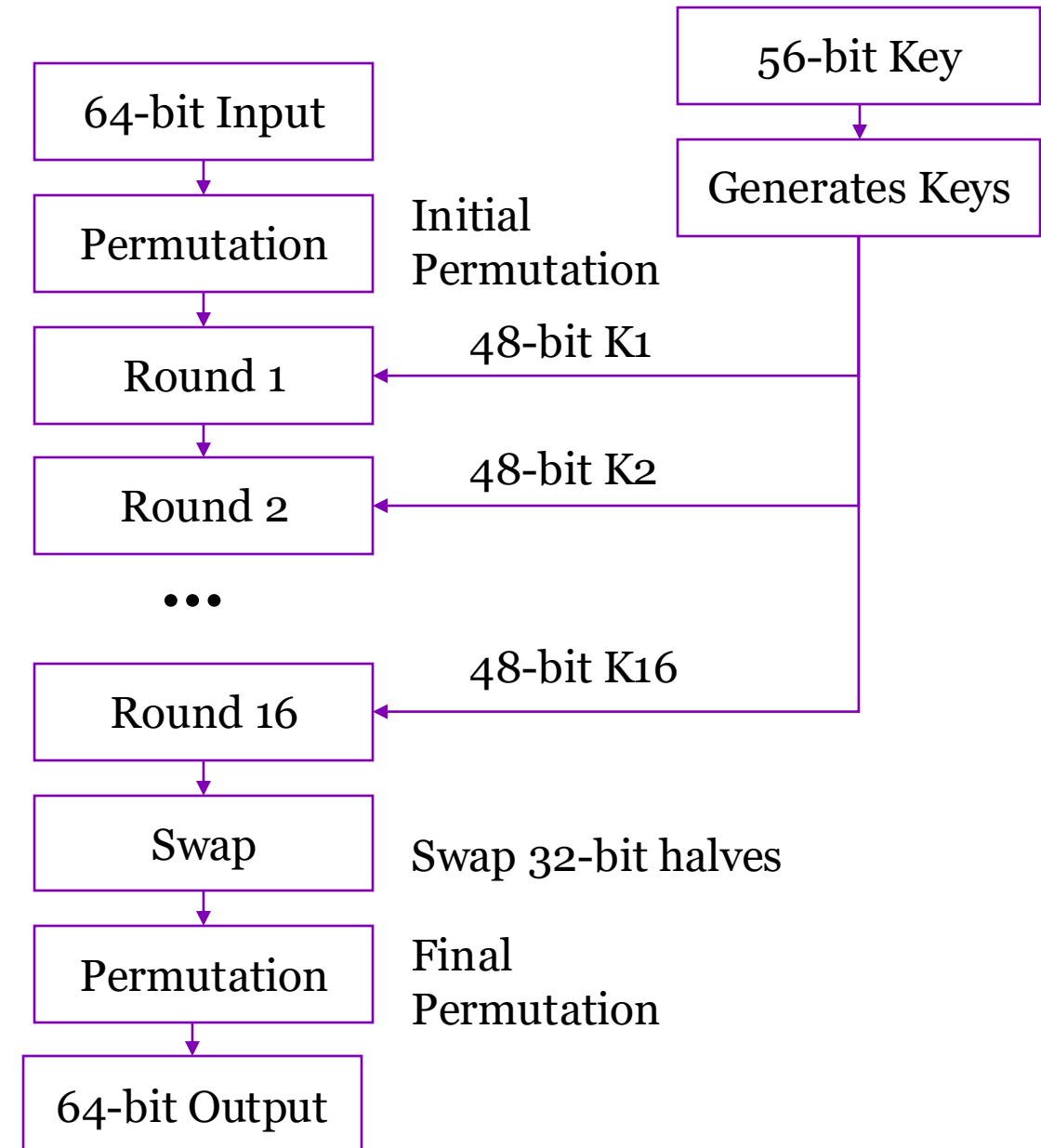
UNIVERSITY OF
WATERLOO

FACULTY OF
ENGINEERING



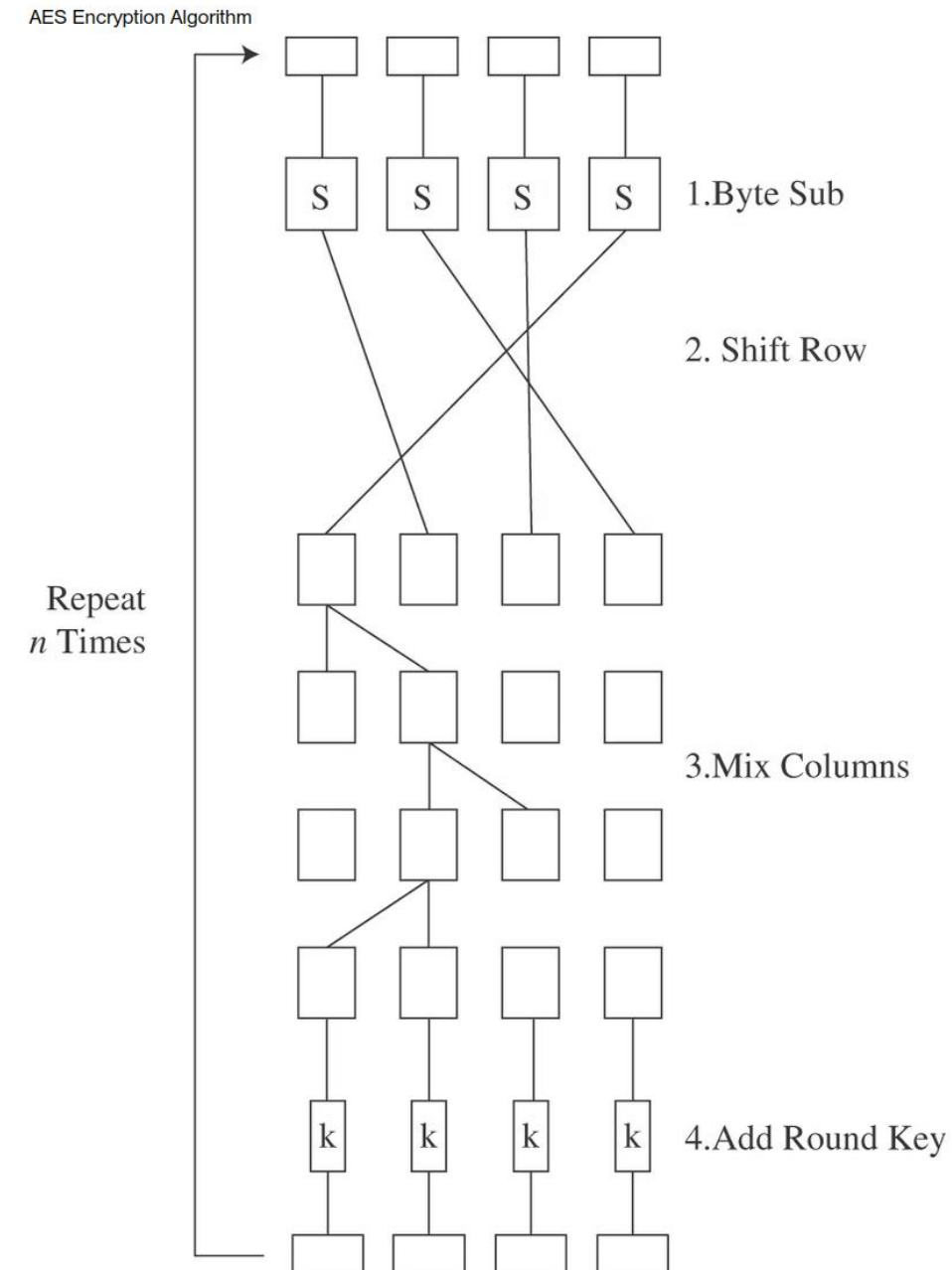
Data Encryption Standard (DES)

- Symmetric-key algorithm using 56 bit keys (64 bit initial but 8 bits are parity)
- Blocks of 64 bits
- Developed in 1970s at IBM
- Approved by NSA (after key length shortened) leading to quick adoption
- January 1999, distributed.net and the Electronic Frontier Foundation collaborated to publicly break a DES key in 22 hours and 15 minutes (Wikipedia)



Advanced Encryption System (AES)

- Became a standard in the US in 2001 after a public proposal call by NIST
- Symmetric key block cipher
- Primarily uses substitution, transposition, the shift, exclusive OR, and addition
- Can use 128, 192, 256 bit keys, and larger keys are possible
 - Key length impacts the number of rounds, longer key, more rounds



Advanced Encryption System (AES)

- Became a standard in the US in 2001 after a public proposal call by NIST
- Symmetric key block cipher
- Primarily uses substitution, transposition, the shift, exclusive OR, and addition
- Can use 128, 192, 256 bit keys, and larger keys are possible
 - Key length impacts the number of rounds, longer key, more rounds

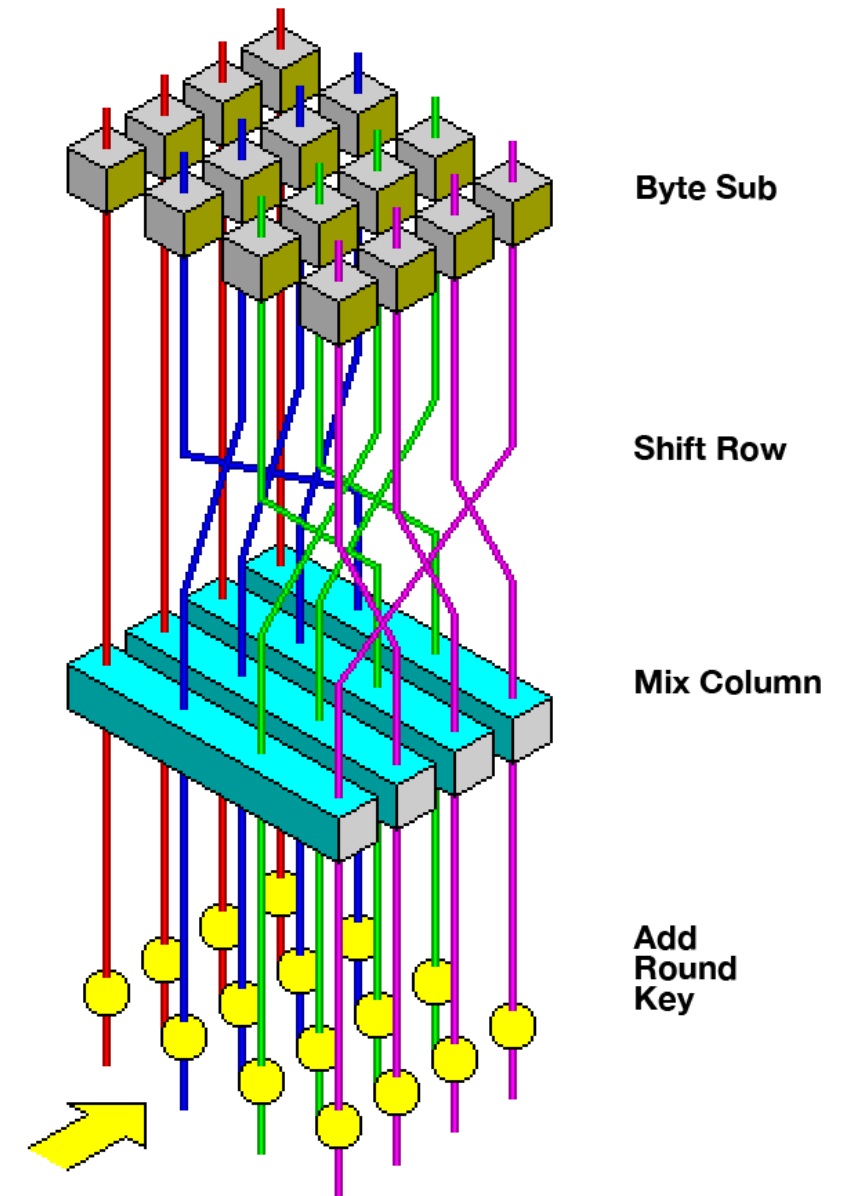


Diagram of the stages of the AES round function
John Savard -- Wikimedia

PUBLIC KEY CRYPTOGRAPHY

Symmetric ciphers

- The prior examples are all symmetric ciphers where the same key is used for encryption and decryption
- Sharing the key can be problematic



Leo Marks with letter One Time Pad written on silk. These were used during WWII by spies. Letters unraveled after use to prevent decryption of earlier messages if captured.



Asymmetric ciphers

- Different keys are used to encrypt and decrypt
- Asymmetric ciphers are less common as they rely on trapdoor functions



Trapdoor one-way function

- A function that is easy to compute but hard to impossible to reverse
- Classic example: Generate two prime numbers p and q and compute their product $N=q \cdot p$



We can use trapdoor functions to securely create a shared key between two people communicating publicly.

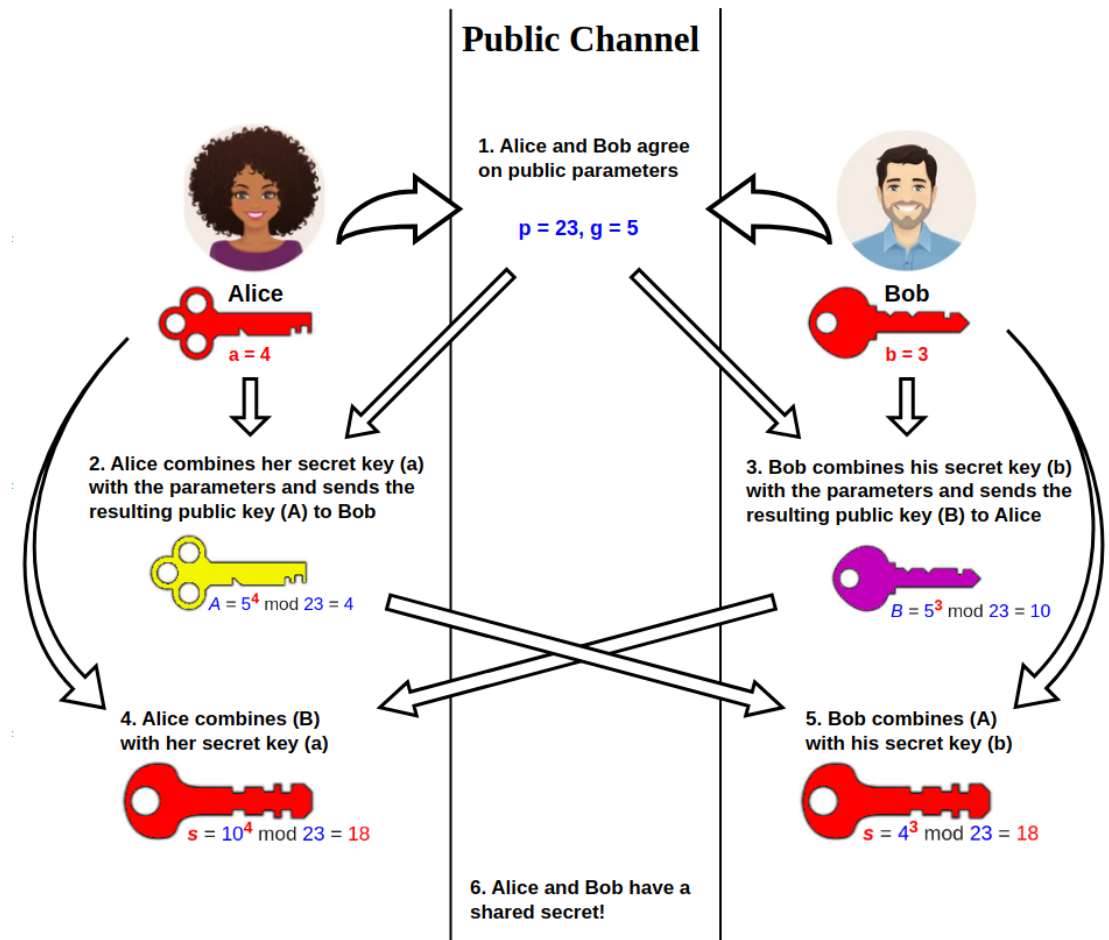
Diffie-Hellman key exchange (Invented 1976... or maybe 1969)

- Allows two entities to agree on a secret key while communicating publicly.
- Protocol uses the multiplicative group of integers modulo p where p is prime and g is a primitive root modulo p .

Primitive Root:

The number 3 is a primitive root modulo 7^[5] because

$$\begin{aligned}
 3^1 &= 3^0 \times 3 \equiv 1 \times 3 = 3 \equiv 3 \pmod{7} \\
 3^2 &= 3^1 \times 3 \equiv 3 \times 3 = 9 \equiv 2 \pmod{7} \\
 3^3 &= 3^2 \times 3 \equiv 2 \times 3 = 6 \equiv 6 \pmod{7} \\
 3^4 &= 3^3 \times 3 \equiv 6 \times 3 = 18 \equiv 4 \pmod{7} \\
 3^5 &= 3^4 \times 3 \equiv 4 \times 3 = 12 \equiv 5 \pmod{7} \\
 3^6 &= 3^5 \times 3 \equiv 5 \times 3 = 15 \equiv 1 \pmod{7}
 \end{aligned}$$



Epachamo via Wikimedia Commons

Trapdoors can also be used to do cryptography using two keys (asymmetric).

I am going to start by explaining at a high level, then we will discuss how it is done.

Encryption properties we want:

1. The communication between you and the other party is **confidential** and has **not been changed (integrity)**
 - No one can read what you sent
 - No one can change what you sent
2. **Knowing who** you are communicating with (authenticity)
 - 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
- **What one key encrypts only the other key can decrypt**

Public

- Public keys are given out to everybody

Private

- Private keys are kept private

- k_{PRIV} can encrypt and k_{PUB} can decrypt

$$P = D(k_{\text{PUB}}, E(k_{\text{PRIV}}, P))$$

- k_{PUB} can encrypt and k_{PRIV} can decrypt

$$P = D(k_{\text{PRIV}}, E(k_{\text{PUB}}, P))$$

My public key



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

Version: GnuPG v2

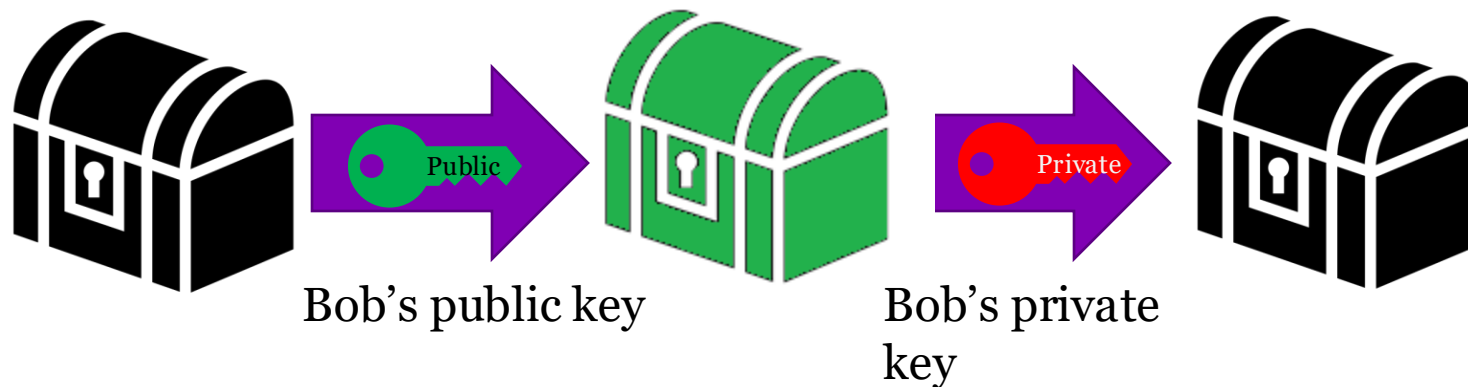
```
mQENBFHMcGABCAC9WrYDO6K2L3VHy14eHN6suHLqMpJ+SO+IUTuLEVNuzIoXAUXH
KozHejfV/9XoG8j933ZtsXKCog3aMESeoEoz6fNGfolvaCe5B4jwqoJt8NHwb5L
B2dnqoCplgXcN2GJxfHHUaf27COSobCJxPMeshU4ZHKke+g6DatmiEtBpVp41Ot
1zxdmMQkgb2H2xw28RYfykdDoueteIkOrFLrCy9ZF9KdMhA1eBH94KnwI QshdiZR
QYEX25+M8cKCb++Rc9H6an7EG9WHOFRW4oUsY52OfveOyfQPzkkRto7u2339hvHo
B/h+7xLM6FQbOUZQ9BD5w7IQHgYtXJVsUjodABEBAAgoIkthbWkgVmFuaVWvHIDxr
dmFuaWVhQGluZi5lZC5hYy51az6JAT8EEwELACkFALYKYvECGyMFCQlMAYAHcwkI
BwMCAQYVCAIJCgsEFgIDAQIeAQIXgAAKCRCTdsxl9/HZffG+ CACShuKxje3QAqew
GWh8K4gCdiYoxDqJwq3PHxmyhZmQeN/1a1KcOrIj12b+Q75/5t+EgXOHPRoP1xfG
lZ6zOEpf6A18fXx3JgQZdwPD0jtBiWNpOyMeBGTgIvEYg3so2VueQoeXcq3dbYp
5vstVtD+TKHq5CioT75P2bzYq/XLT5aIbNQhQDPcToDgBRH+FvqsRXr7yeaf
JaPnxXo+1L33t2QY9zctiGyebwrvHMrIPBJ2VYCDzQk7JuQ5eFh4ZhsMgOmzLQD4
YiGr5weIMFwAvxZOARxAgVf48jiWvrXuJ8YfHWSohESeNOCYCzP8q2oJwwE26T
lpdtrwCqtB1LYW1pIFZhbmlYSA8a2FtaUB2YW5pZWUy9tPobkBgQTAQIALAlb
IwUJCWYBgAcLCQgHAWIBBhULAgKcQWQAgaMBAh4BAheABQJWCmMeAhkBAaoJEJN2
zGX38dl9JJAIAIWorxIYsrnKS6CbW8MgTxxTDOXA Ct1b7FoWoQZHskIUqhEcEa+
XBYibiA5uHaatLfyeXaD3qMEoZnQHoyMGEoGKuooWsbhfoQzHPgwzRLkdii75M
BibawwoKWoVB9e4AkMakXJcNf5BXeo6AHLRL2v15V205DikVnlCRXocKtu8b7LnkM
eLn7oLobr1de1uyKoNzbSnO/vpKDJPo/EY5yUeV9oIypZy/6wFQBehg1sXye6znO
9wb9uUs9+/P8pz4JILMDSevjfT7zSRSL/YP3fOfZ6N4bc+KODwPM7u5Iyoeu9zh
pzibv3ge7VhH2xIWz8vYz/2xT1345tWRRMOJAhwEEwECAAyFALTnSpEACgkQjyxM
p99tBt2B8A/+OpIzOsQbQJB8yxti4l7PpD1weJDF3a81Vhm7JyXE/Xy66ypfdt3w
XmFRUulrwezYiNebWNCrQHHzQvRv/VJwjbTUX+Q3HsjkKlHbE7iCiQXXtTRkoEny
2nu dcjGI2vo3C3B2JCucEw6esF1x79PI/1Pv2+6tgUBKmDfOpsB2vbtqrHnmAYKL
4lQBFH1YSJgnzwo2JkhhocHdF9oZem1eMeiDeeVkh63893N8Swk5fBKdTj+SKZ/L
rQElBBlpMR9BmeY6bPvWRuyevKonIMR8oG9iFABxjTpWBL8aGk6EeVK5EqYDgVkd
ZlarK84r+KU1KD5lfgOCN7nhwgy7VI meE68caZHSRiPWZP1fVVMhydiRjv8WsoUs6
InFvU3nxH+ZYthPbYoT86leGSchBT5K/fbQvbjhrRTbTfwwjzSifb9efWylDi994
nzP6cNorir3GIpsT8gPgBB2/NjxaWiM6y3X1az1vRnsunQHuyKkFWPZwnEvDJYaC
NN/3jWcbhLFwKBDsaHps2+1meFPooJFvNetz2bjT9a9pXaQ6KhOmo5DnhLcaV97
bFBpsUuBgAYZTSSo5x1RdXHqpEbgap8dtuHhVvJw9QYDQBjroK4aKyG9qqMD8cta
Pl/FAdyAqWH8Nw9efqAK+RQxSVUaue9BYEnbIRpsDK6MkP3YMFmu5ki5AQoEUcxy
AAEIALyXYy8G2ZaTDJpdGcRhmIqOOSUlzPV7/5E5BbYKBNu4KU3nX+JLvcF5jxPQ
42c7i/WRVxE1BJTiarKGsEvCi94TXXSIUKAt3T1oGBtXmGvqbGBq8ljSGl1UTwdF
5yu5oJyRSf2fQRND6P/2eHNXejDUdtvhUXIU8h9MuUO/ipDoDnwIvMnAATJHA+R
Zqw6oNpyjRGzvr3i uWUw4PtyJDI3ELAFkbp/NAc5TtUvHRHNOwnpldJhMzHuB
QQb3G/EsCn2PQZ5w5SDzavF2SpvQfDqxYpDaTLAXtF+wsJL5iaUjxwRgJPodbCZf
2Tozd7h9MXtGJDlPKJ8eLG8ogcMAEQEAAYkBJQQYAQIADwUCUcxyAAIbDAUJCWYB
gAAKCRCTdsxl9/HZfS+hB/9BJqSmIgcOHFXnb1PVikxekzL8+WVm5Pk/EgMQSLZ2
HX4p3ial5PEPEYgUw9YnaG4ioodwJGw5/daTWrrTzcnKd8YqoP+DUOt96HZDSu3m
mCzE9NVAQYboFbVmGOxoeo627UBSvFqaXvAxBDYkoR8BoTnKhrQFwXkZVb3ohKwD
TgAFjOGlZiE6uAdST231tFaqobizYfe5AVXRqro2oxBqNbaJNqs3SWoD83iSyvdv
lIOBx83/Rogg7hUkI6F2vzXicWmUwFSXRggCSbLosHsP6isBWwvIHeRmna/aQab
YKG3gbV9iyzAS31gbogVLAZqNSWhp8vVIEE28Fyf/Ed
```

=x5FK

-----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

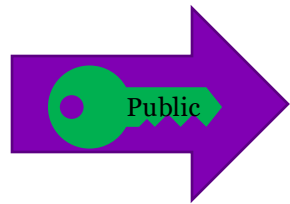
```
mQENBFHMcGABCAC9WrYDO6K2L3VHy14eHN6suHLqMpJ+SO+IUTuLEVNuzIoXAUXH
KozHejFV/9XoG8j93ZtszXKCog3aMESeoEoz6fNGfolvaCe5B4jwqoJt8NHw5L
B2dnqoCplgXcN2GJxfEHHUaf27COSobCJxPMeshU4ZHKke+g6DatmiEtBpVp41Ot
1zgxMqkGb2H2xw28RYfykdDoueteIkOrFLrCy9ZF9KdMhA1eBH94Knw1QshdiZR
QYEX25+M8cKCb++Rc9H6an7EG9WHOFrW40UsY52OfveOyfQPzkkRto7u2339hvHo
B/h+7xLM6FQbOUZQ9BD5w7IQHgYtXJVsUjodABEBAAGOIktbWkgVmFuaWVhIDxr
dmFuaWVhQGluZi5lZC5hYy51az6JAT8EEwEIAckFAIKYvECGyMFCQlMAYAHcwkI
BwMCAQYVYCAIJCgsEFgIDAQIeAQIXgAAKCRCTdSxlg/HZffG+CACShuKxje3QAqew
GWh8K4gCdiYoxDqJwq3PHxmyhZmQeN/1a1KcOrIj12b+Q75/5t+EgXOHpRoPIxfG
lZ6zOEpf6A18fXx3JgQZdwPD0jtBiWNpOyMeBGTgIvEYg3so2VueQoeXcq3dbYp
5vstVxtD+TKHq5CioT75P2bzYq/XLT5aIbNqhQDPcT0oDgbRH+FvqsRXr7yeaef
JaPnxXo+1L33t2QY9zctiGyebwrvHMrIPBJ2VYCDzQk7JuQ5eFh4ZhsMgOmzLQD4
YiGr5weIMFwAvxZOARxEagVf48jiWvrXuJ8YfHWSohESeNOCYCp8q2olwwE26T
lpdtrwCqtB1LYW1pIFZhbmlYSA8a2FtaUB2YW5pZWUy9tPobkBgQTAQIALAlB
IwUJCWYBgAcLCQgHAWIBBHUIAgKcKwQWAGMBAh4BAheABQJWCmMeAhkBAAoJEJN2
zGX38dl9JJAIAIWorxIYsrnKS6CbW8MgTxxTDOXA Ct1b7FoWoQZHskIUqhEcE+a
XBYibiA5uHaatLfyeXaD3qMEoZnQHoyMGEoGKu0owWsbhfoQzHPgwzRLkDii75M
BfbawwoKWoVB9e4AkMakXJcNf5BXeo6AHL2v15V205DikVnlCRXocKtu8b7LnmK
eLn7oLobr1deIuyKoNzbSnO/vpKDJPo/EY5yUeV9oIypZy/6wFQBehg1sXye6znO
9wb9uUsu9+/P8pz4JILMDSevjfT7zSRSL/YP3fOfZ6N4bc+KODwPM7u5Iyoeguzh
pzibv3ge7VhH2xIWz8vYZ/2xT1345tWRRMOJAhwEEwECAAyFALTnSpEACgkijyxM
p99tBt2B8A/+OpIzOsQbQJB8yxti4l7PpD1weJDF3a81Vhm7JyXE/Xy66ypfdt3w
XmFRUulrwezYiNebWNCrQHHzQvRv/VJwbjTUX+Q3HsjkKlHbE7CiQXXtTRkoEny
2nu dcjGI2vo3C3B2JCucEw6esF1x79PlPv2+6tgUBKmDfOpsB2vbtqrHnmAYKL
4lQBFH1YSJgnzwo2JkhhocHdF9oZem1eMeiDeeVkh63893N8Swk5fBKdTj+SKZ/L
rQElBBlpMR9BmeY6bPvWRuyvKkonIMR8oG9iFABxjTpWBL8aGk6EeVK5EqYDgVkd
ZlarK84r+KU1KD5lfgOCN7nhwgy7VI meE68caZHSRiPWZP1fVVMhydiRjv8WsoUs6
InfVU3nxH+ZYthPhYoT86leGSchBT5K/fbQvbjhrRTbTFwvzSifb9efWylDi994
nzP6cNorir3GIpsT8gPGBB2/NjxaWiM6y3X1az1vRnsunQHuyKkFWPZwnEvDJYaC
NN/3jWcbhLFwKBDsaHps2+1meFPooJFvNetz2bjT9a9pXaQ6KhOmo5DnhLcaV97
bFBpsUuBGaYZTSSo5x1RdXHqPebgap8dtuHhVvJw9QYDQBjroK4aKyG9qqMD8cta
Pl/FAdyAqwH8Nw9efqAK+RQxSVUaue9BYEnbIRpsDK6Mkp3YMFmu5ki5AQoEUcxy
AAEIALyXYy8G2ZaTdJpdGcRhmIqOOSUlzPV7/5E5BbYKBNu4KU3nX+JLvcF5jxPQ
42c7i/WRVxE1BJTiarKGsEvCi94TTXSIUKAt3T1oGBtXmGvqbGBq1BSgl1UTwdF
5yu5oJyRSf2fQrND6P/2eHNXejDUtdvhUXIU8h9MuUO/ipDoDnwIvMnAtJHA+R
Zqw6oNpyjRGzvr3iUWUwe4PtyJDI3ELAFkbp/NAC5TtUvHRHNOwnpldJhM5zHuB
QQb3G/EsCn2PQZ5w5SDzavF2SpvQfDqxYpDaTLAXtF+wsJL5iaUjxwRgJPodbCZf
2Tozd7h9MXtGJdIPKJ8eLG8ogcMAEQEAAYkBJQQYAQIADwUCUcxyAAIbDAUJCWYB
gAAKCRCTdSxlg/HZfs+hB/9BJqSmIgcoHFXnb1PVIKxekzL8+WVW5Pk/EgMQSLZ2
HX4p3ial5PEPEYgUw9YnaG4ioodwJGw5/d4TWRrTzcnKd8YqoP+DUOt96HZDSu3m
mCzE9NVAQYboFbVmGOXoeo627UBSvFqaXvAXBDYkoR8BoTnKhRQfWxKzVb3ohKwD
TgAFjOGlZiE6uAdST231tFaqobizYfe5AVXRqro2oxBqNbaJNqs3SWoD83iSyvdv
lloBx83/Rogg7hUkI6F2vzXicWmUwFSXRggCSbLosHsP6isBWwvlHeRmna/aQab
YKG3gbV9jyczAS31gbogVLAZqNSWhp8vVIEE28Fyf/Ed
```

=x5FK

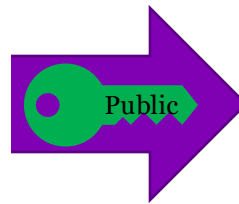
-----END PGP PUBLIC KEY BLOCK-----

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



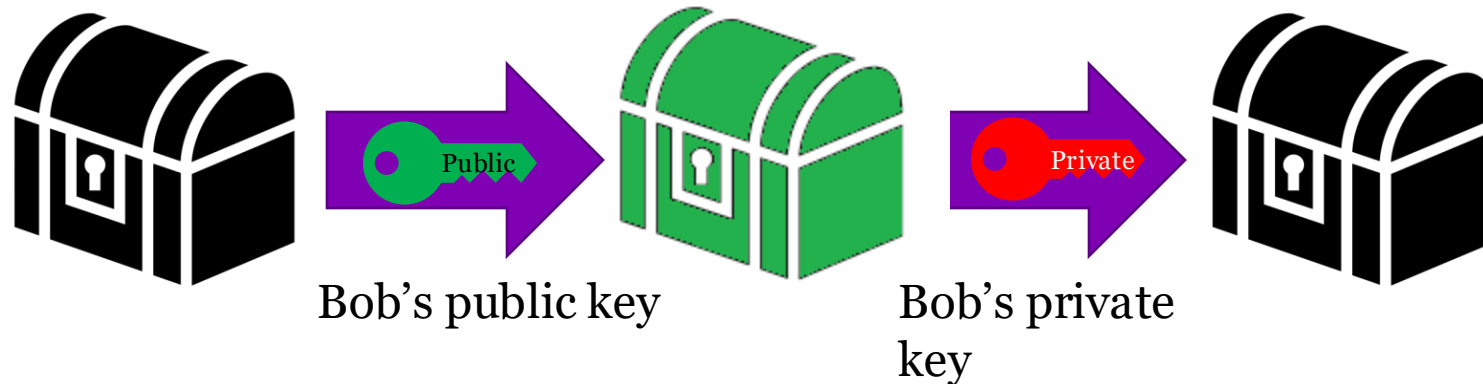
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

```
mQENBFHMcGABCAC9WrYDO6K2L3VHy14eHN6suHLqMpJ+SO+IUTuLEVNuzIoXAUXH
KozHejFV/9XoG8j933ZtszXKCog3aMESeoEoz6fNGfolvaCe5B4jwqoJt8NHwb5L
B2dnqoCplgXcN2GJxfEHHUaf27COSobCJxPMeshU4ZHKke+g6DatmiEtBpVp41Ot
1zgxMqKgb2H2xw28RYfykdDoueteIkOrFLrCy9ZF9KdMhA1eBH94Knw1QshdiZR
QYEX25+M8cKCb++Rc9H6an7EG9WHOFRW40UsY52OfveOyfQPzkkRto7u2339hvHo
B/h+7xLM6FQbOUZQ9BD5w7IQHgYtXJVsUjodABEBAAgOIkthbWkgVmFuaVWvHIDxr
dmFuaWVhQGluZi5lZC5hYy51az6JAT8EEwELACkFALYKYvECGyMFCQlMAYAHcwkI
BwMCAQYVYCAIJGsgEFgIDAQIeAQIXgAAKCRCTdsxl9/HZffG+CACShuKxje3QAqew
GWh8K4gCdiYoxDqJwq3PHxmyhZmQeN/1a1KcOrIj12b+Q75/5t+EgXOHpRoPIxfG
lZ6zOEpf6A18iFXx3JgQZdwPD0jtBiWNpOyMeBGTgIvEYg3so2VueQoeXcq3dbYp
5vstVxtD+TKHq5CioT75P2bzYq/XLT5aIbNqhQDPcToDgBRH+FvqsRXr7yeaef
JaPnxXo+1L33t2QY9zctiGyebwrvHMrIPBJ2VYCDzQk7JuQ5eFh4ZhsMgOmzLQD4
YiGr5weIMFwAvxZOARxEagVf48jiWvrXuJ8YfHWSohESeNOCYCp8q2olwwE26T
lpdtrwCqtB1LYW1pIFZhbmlYSA8a2FtaUB2YW5pZWUy9tPokBQgQTAQIALAlB
IwUJCWYBgAcLCQgHAWIBBHUIAgKcKwQWAgMBAh4BAheABQJWCmMeAhkBAAoJEJN2
zGX38dl9JJAIAIWorxIYsrmKS6CbW8MgTxxTDOXA Ct1b7FoWoQZHskIUqhEcE+a
XBYibiA5uHaatLfyeXaD3qMEoZnQHoyMGEoGKuooWsbhfoQzHPgwzRLkDii75M
BfbawwoKWoVB9e4AkMakXJcNf5BXeo6AHL2v15V205DikVnlCRXocKtu8b7LnmK
eLn7oLobr1de1uyKoNzbSnO/vpKDJPo/EY5yUeV9oIypZy/6wFQBehg1sXye6znO
9wb9uUsu9+/P8pz4JILMDSevjfT7zSRSL/YP3fOfZ6N4bc+KODwPM7u5Iyoeguzh
pzibv3ge7VhH2xIWz8vYZ/2xT1345tWRRMOJAhwEEwECAAyFALTnSpEACgkQjyxM
p99tBt2B8A/+OpIzOsQbQJB8yxti4l7PpD1weJdf3a81Vhm7JyXE/Xy66ypfdt3w
XmFRUulrwezY1NebWNCrQHqZvRv/VJwjbTUX+Q3HsjIkKlHbE7CiQXxtTRkoEny
2nuGjGI2vo3C3B2JCucEw6esF1x79PI/1Pv2+6tgUBKmDfOpsB2vbtqrHnmAYKL
4lQBFH1YSJgnzwo2JkhhocHdF9oZem1eMeiDeeVkh63893N8Sww5fBKdTj+SKZ/L
rQElBBlpMR9BmeY6bPvWRuyvKkonIMR8oG9iFABxjTpWBL8aGk6EeVK5EqYDgVkd
ZlarK84r+KU1KD5lfgOCN7nhwgy7VI me68caZHSRiPWZP1fVVMhydiRjv8WsoUs6
InfVU3nxH+ZYthPbYoT86leGSchBT5K/fbQvbjhrRTbTFwvzSifb9efWylDi994
nzP6cNorir3GIpsT8gPGBB2/NjxaWiM6y3X1az1vRnsunQHuyKkFWPZwnEvDJYaC
NN/3jWcbhLFwKBDsaHps2+1meFPooJFvNetzp2bjT9a9pXaQ6KhOmo5DnhLcaV97
bFBpsUuBGaYZTSSo5x1RdXHqpEbgap8dtuHhVvJw9QYDQBjroK4aKyG9qqMD8cta
Pl/FAdyAqWH8Nw9efqAK+RQxSVUaue9BYEnbIRpsDK6MkP3YMFmu5ki5AQoEUcxy
AAEIALYXYy8G2ZaTdJpdGcRhmIqOOSUlpV7/5E5BbYKBNu4KU3nX+JLvcF5jxPQ
42c7i/WRVxE1BJTiarKGsEvCi94TtXSIUKat3T1oGBtXmGvqbGBqbljSGl1UTwdF
5yu5oJyRSf2fQRND6P/2eHNXejDUtdvhUXIUt8h9MuUO/ipDoDnwIvMnAATJHA+R
Zqw6oNpyjRGzvr3iUWUwe4PtyJDI3ELAFkbp/NAC5TtUvHRHNOwnpldJhM5zHuB
QQb3G/EsCn2PQZ5w5SDzavF2SpvQfDqxYpDaTLAXtF+wsJL5iaUjxwRgJPodbCZf
2Tozd7h9MXtGJdIPKJ8eLG8ogcMAEQEAAYKBJQQYAQIADwUCUcxyAAIbDAUJCWYB
gAAKCRCTdsxl9/HZfs+hB/9BJqSmIgcOHFXnb1PVikXekzL8+WVM5Pk/EgMQLZ2
HX4p3ial5PEPcYgUw9YnaG4ioodwJGw5/daTWrrTzcnKd8YqoP+DUot96HZDSu3m
mCzE9NVAQYboFbVmGOXoe627UBSvFqaXvAXBDYkoR8BoTnKhrQFwXkZVb3ohKwD
TgAFjOGlZiE6uAdST231tFaqobizYfe5AVXRqro2oxBqNbaJNqsgSWoD83iSyvdv
lloBx83/Rogg7hUkI6F2vzXicWmUwFSXRggCSbLosHsP6isBWwvIHeRmna/aQab
YKG3gbV9jyczAS31gbogVLAZqNSWhp8vVIEE28Fyf/Ed
```

=x5FK
-----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
B2dnqoCplgXcN2GJxfEHHUaf27COSobCJxPMeshU4ZHKke+g6DatmiEtBpVp41Ot
1zgxMqkGb2H2xw28RYfykdDoueteIkOrFLrCy9ZF9KdMhA1eBH94Knw1QshdiZR
QYEX25+M8cKCb++Rc9H6an7EG9WHOFrW40UsY52OfveOyfQPzkkRto7u2339hvHo
B/h+7xLM6FQbOUZQ9BD5w7IQHgYtXJVsUjodABEBAAgOIkthbWkgVmFuaVWVhIDxr
dmFuaWVhQGluZi5lZC5hYy51az6JAT8EEwELACkFALYKYvECGyMFCQlMAYAHcwkI
BwMCAQYVYCAIJCgsEFgIDAQIeAQIXgAAKCRCTdSxlg/HZffG+CACShuKxje3QAqew
GWh8K4gCdiYoxDqJwq3PHxmyhZmQeN/1a1KcOrIj12b+Q75/5t+EgXOHpRoPIxfG
lZ6zOEpf6A18fXx3JgQZdwPD0jtBiWNpOyMeBGTGIvEYg3so2VueQoeXcq3dbYp
5vstVxtD+TKHq5CioT75P2bzYq/XLT5aIbNqHqDPcToDgBRH+FvqsRXr7yeaef
JaPnxXo+1L33t2QY9zctiGyebwrvHMrIPBJ2VYCDzQk7JuQ5eFh4ZhsMgOmzLQD4
YiGr5weIMFwAvxZOARxEagVf48jiWvrXuJ8YfHWSohEScNOCYCp8q2olwwE26T
lpdtrwCqtB1LYW1pIFZhbmlYSA8a2FtaUB2YW5pZWUy9tPokBQgQTAQIALAlB
IwUJCWYBgAcLCQgHAWIBBHUIAgKcKwQWAGMBAh4BAheABQJWCmMeAhkBAAoJEJN2
zGX38dl9JJAIAIWorxIYsrnKS6CbW8MgTxxTDOXA Ct1b7FoWoQZHskIUqhEcE+a
XBYibiA5uHaatLfyeXaD3qMEoZnQHoyMGEoGKuooWsbhfoQzHPgwzRLkDii75M
BfbawwoKWoVB9e4AkMakXJcNf5BXeo6AHLRL2v15V205DikVnlCRXocKtu8b7LnmK
eLn7oLobr1deIuyKoNzbSnO/vpKDJPo/EY5yUeV9oIypZy/6wFQBehg1sXye6znO
9wb9uUsu9+/P8pz4JILMDSevjfT7zSRSL/YP3fOfZ6N4bc+KODwPM7u5Iyoeguzh
pzibv3ge7VhH2xIWz8vYZ/2xT1345tWRRMOJAhwEEwECAAyFALTnSpEACgkQjyxM
p99tBt2B8A/+OpIzOsQbQJB8yxti4l7PpD1weJdf3a81Vhm7JyXE/Xy66ypfdt3w
XmFRUulrwezYiNebWNCrQHHzQvRv/VJwbjTUX+Q3HsjkKlHbE7CiQXXtTRkoEny
2nu dcjGI2vo3C3B2JCucEw6esF1x79PI/Pv2+6tgUBKmDfOpsB2vbtqrHnmAYKL
4lQBFH1YSJgnzwo2JkhhocHdF9oZem1eMeiDeeVkh63893N8Swk5fBKdTj+SKZ/L
rQElBBlpMR9BmeY6bPvWRuyvKkonIMR8oG9iFABxjTpWBL8aGk6EeVK5EqYDgVkd
ZlarK84r+KU1KD5lfgOCN7nhwgy7VI meE68caZHSRiPWZP1fVVMhydiRjv8WsoUs6
InFVU3nxH+ZYthPbYoT86leGSchBT5K/fbQvbjhrRTbTFwvzSifb9efWylDi994
nzP6cNorir3GIpsT8gPGBB2/NjxaWiM6y3X1az1vRnsunQHuyKkFWPZwnEvDJYaC
NN/3jWcbhLFwKBDSaHps2+1meFPooJFvNetz2bjT9a9pXaQ6KhOmo5DnhLcaV97
bFBpsUuBGaYZTSSo5x1RdXHqPebgap8dtuHhVvJw9QYDQBjroK4aKyG9qqMD8cta
Pl/FAdyAqwH8Nw9efqAK+RQxSVUaue9BYEnbIRpsDK6Mkp3YMFmu5ki5AQoEUcxy
AAEIALyXYy8G2ZaTdJpdGcRhmIqOOSUlvP7/5E5BbYKBNu4KU3nX+JLvcF5jxPQ
42c7i/WRVxE1BJTiarKGsEvCi94TTXSIUKAt3T1oGBtXmGvqbGBqB8ljSGl1UTwdF
5yu5oJyRSf2fQRND6P/2eHNXejDUtdvhUXIU8h9MuUO/ipDoDnwIvMnAATJHA+R
Zqw6oNpyjRGzvr3iUWUwe4PtyJDI3ELAFkbp/NAC5TtUvHRHNOwnpldJhM5zHuB
QQb3G/EsCn2PQZ5w5SDzavF2SpvQfDqxYpDaTLAXtF+wsJL5iaUjxwRgJPodbCZf
2Tozd7h9MXtGJdIPKJ8eLG8ogcMAEQEAAYkBJQQYAQIADwUCUcxyAAIbDAUJCWYB
gAAKCRCTdSxlg/HZfs+hB/9BJqSmIgcoHFXnb1PVIKxekzL8+WVM5Pk/EgMQSLZ2
HX4p3ial5PEPEYgUw9YnaG4ioodwJGw5/d4TWRrTzcnKd8YqoP+DUot96HZDSu3m
mCzE9NVAQYb0FbVmGOXoeo627UBSvFqaXvAXBDYkoR8BoTnKhrQFwXkZVb3ohKwD
TgAFjOGlZiE6uAdST231tFaqobizYfe5AVXRqro2oxBqNbaJNqs3SWoD83iSyvdv
lloBx83/Rogg7hUkI6F2vzXicWmUwFSXRggCSbLosHsP6isBWwvIHeRmna/aQab
YKG3gbV9jyczAS31gbogVLAZqNSWhp8vVIEE28Fyf/Ed
```

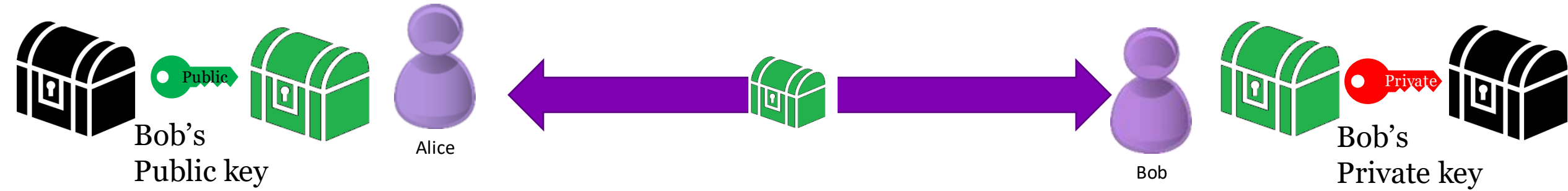
=x5FK

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

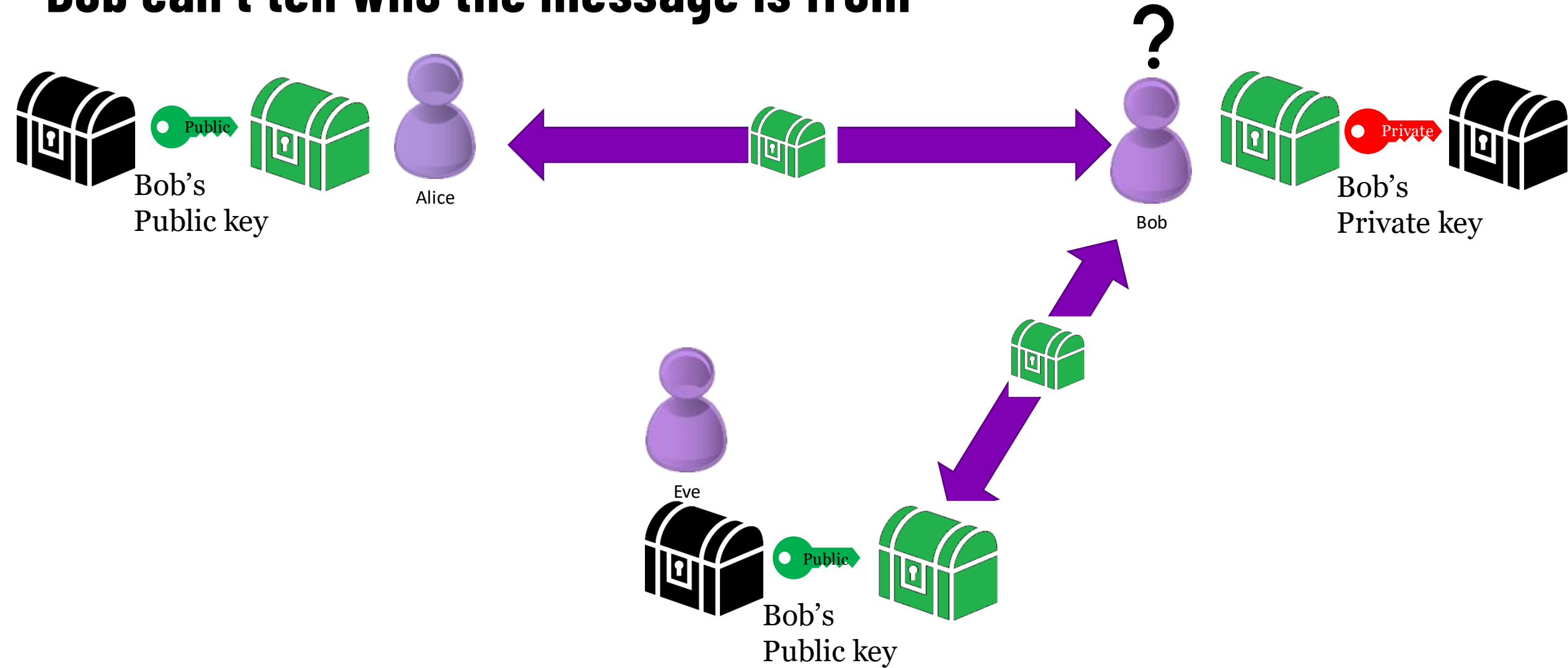
Encryption properties we want:

1. The communication between you and the other party is **confidential** and has **not been changed (integrity)**
 - 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

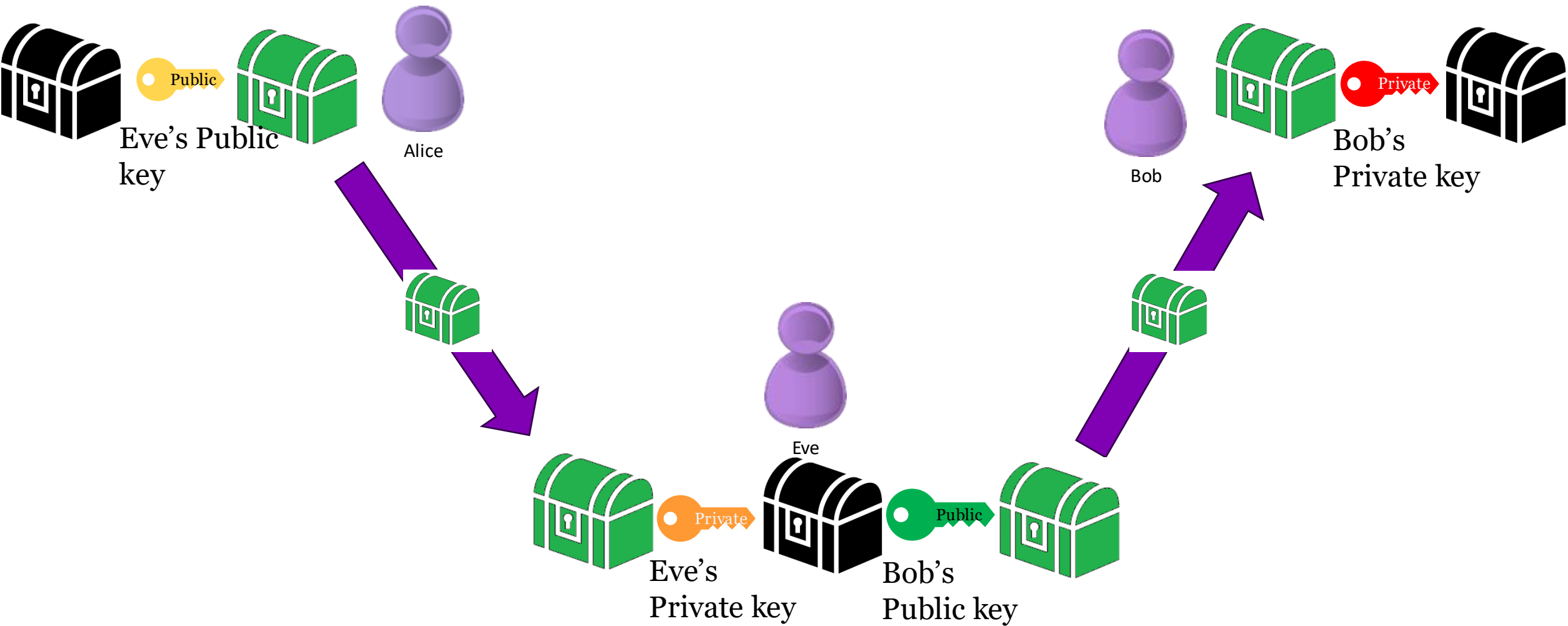
Bob can't tell who the message is from



Bob can't tell who the message is from



Full Man in the Middle (MITM)



Vital to keep private keys private

- The FBI convinced the system administrator to switch out the private key for one the FBI knew
- FBI was able to listen in on all the chats and got lots of evidence

Security

Who cracked El Chapo's encrypted chats and brought down the Mexican drug kingpin? Er, his IT manager

Feds flipped techie and recorded hundreds of calls

By [Kieren McCarthy](#) in [San Francisco](#) 9 Jan 2019 at 21:33

71

SHARE ▼



In an extraordinary twist, it was revealed on Tuesday that the man most likely responsible for bringing drug kingpin "El Chapo" Joaquin Guzman to justice was none other than his sysadmin.

Vital to keep private keys private

- The FBI convinced the system administrator to switch out the private key for one the FBI knew
- FBI was able to listen in on all the chats and got lots of evidence
- How? A high ranking drug trafficker forgot his password and called the admin unencrypted. After FBI heard the conversation they thought the admin might like some protection.

But the drug trafficker isn't happy, complaining about having to get the computer himself, and about the long password needed to get into a different machine: A situation that every sysadmin on the globe will recognize. Except with one big difference - your boss is unlikely to track you down and kill you if you upset him.

"You didn't send me the engineer to install my machine. So, then, it's all your fault," Jorge Cifuentes complained. "No!" responded to Rodriguez.

"It's all your fault."

"No, Don Jorge, don't stress me out more, man, because..."

"Don't complain that I... what can I do? I haven't been able to do it."

"Hadn't we agreed that you were going to buy a mini computer and you were going to call us to configure it?"

"I'm so busy. I didn't even have time to breathe... I have a computer but, you know that I haven't been able to open it? A Vaio... Do you remember the small Vaio?"

"Yes, sir."

"Good, but that has a very long password."

"Yes, sir."

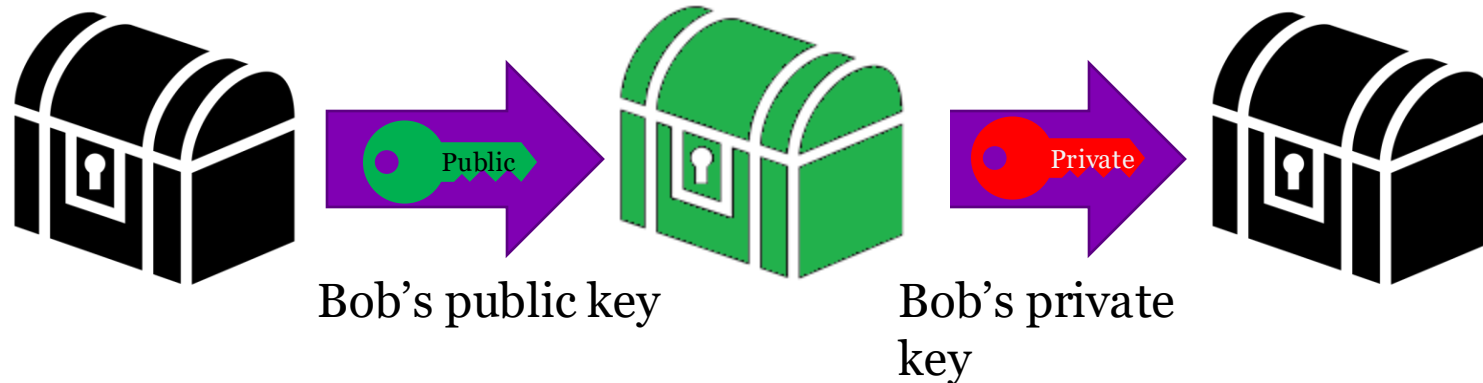
"The long one, that password that you place...is this the password?"

"Yes, sir."

"What a drag! It has symbols and things."

Encryption: 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

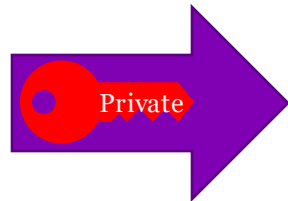
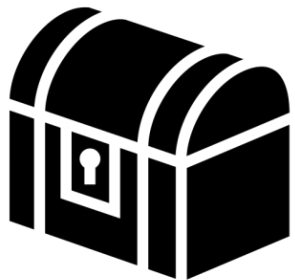
```
mQENBFHMcGABCAC9WrYDO6K2L3VHy14eHN6suHLqMpJ+SO+IUTuLEVnUzIoXAUXH
KozHeJfV/9XoG8j933ZtszXKCog3aMESeoEoz6fNGfolvaCe5B4jwqoJt8NHw5L
B2dnqoCplgXcN2GJxFeHHUaf27COSobCJxPMeshU4ZHKke+g6DatmiEtBpVp41Ot
1zgxDMQkgb2H2xw28RYfykdDoueteIkOrFLrCy9ZF9KdMhA1eBH94Knw1QshdiZR
QYEX25+M8cKCb++Rc9H6an7EG9WHOFrW40UsY52OfveOyfQPzkkRto7u2339hvHo
B/h+7xLM6FQbOUZQ9BD5w7IQHgYtXJVsUjodABEBAAGOIktbWkgVmFuaWVhIDxr
dmFuaWVhQGluZi5lZC5hYy51az6JAT8EEwEIAckFAIKYvECGyMFCQlMAYAHcwkI
BwMCAQYVYCAIJCgsEFgIDAQIeAQIXgAAKCRCTdsxl9/HZffG+CACShuKxje3QAqew
GWh8K4gCdiYoxDqJwq3PHxmyhZmQeN/1a1KcOrIj12b+Q75/5t+EgXOHpRoPIxfG
LZ6zOEpf6A18fXx3JgQZdwPD0jtBiWNpOyMeBGTgIvEYg3so2VueQoeXcq3dbYp
5vstVxtD+TKHq5CioT75P2bzYq/XLT5aIbNqHqDPCTooDgbRH+FvqsRXr7yeaef
JaPnxXo+1L33t2QY9zctiGyebwrvHMrIPBJ2VYCDzQk7JuQ5eFh4ZhsMgOmzLQD4
YiGr5weIMFwAvxZOARxEagVf48jiWvrXuJ8YfHWSohESeNOCYCp8q2olwwE26T
lpdtrwCqtB1LYW1pIFZhbmlYSA8a2FtaUB2YW5pZWUy9tPokBQQTAAIALiAlB
IwUJCWYBgAcLCQgHAWIBBHUIAgkKCwQWAgMBAh4BAheABQJWCmMeAhkBAAoJEJN2
zGX38dl9JJAIAIWorxIYsrnKS6CbW8MgTxxTDOXA Ct1b7FoWoQZHskIUqhEcE+a
XBYibiA5uHaatLfyeXaD3qMEoZnQHoyMGEoGKuooWsbhfoQzHPgwzRLkDii75M
BtbawwoKWoVB9e4AkMakXJcNf5BXeo6AHL2v15V205DikVnlCRXocKtu8b7LnmK
eLn7oLobr1deIuyKoNzbSnO/vpKDJPo/EY5yUeV9oIypZy/6wFQBehg1sXye6znO
9wb9uUsu9+/P8pz4JILMDSevjfT7zSRSL/YP3fOfZ6N4bc+KODwPM7u5Iyoeguzh
pzibv3ge7VhH2xIWz8vYZ/2xT1345tWRRMOJAhwEEwECAAyFALTnSpEACgkQjyxM
p99tBt2B8A/+OpIzOsQbQJB8yxti4l7PpD1weJDF3a81Vhm7JyXE/Xy66ypfdt3w
XmFRUulrwezYiNebWNCrQHHzQvRv/VJwbjTUX+Q3HsjkKlHbE7CiQXXiTRkoEny
2nu dcjGI2vo3C3B2JCucEw6esF1x79PI/Pv2+6tgUBKmDfOpsB2vbtqrHnmAYKL
4lQBFH1YSJgnzwo2JkhhocHdF9oZem1eMeiDeeVkh63893N8Swk5fBKdTj+SKZ/L
rQElBBlpMR9BmeY6bPvWRuyvKkonIMR8oG9iFABxjTpWBL8aGk6EeVK5EqYDgVkd
ZlarK84r+KU1KD5IfgOCN7nhwgy7VI meE68caZHSRIPWZP1fVVMhydiRjv8WsoUs6
InfVU3nxH+ZYthPhYoT86leGSchBT5K/fbQvbjhrRTbTFwvzSifb9efWylDi994
nzP6cNorir3GIpsT8gPGBB2/NjxaWiM6y3X1az1vRnsunQHuyKkFWPZwnEvDJYaC
NN/3jWcbhLFwKBDSaHps2+1meFPooJFvNetz2bjT9a9pXaQ6KhOmo5DnhLcaV97
bFBpsUuBGaYZTSSo5x1RdXHqPEbgap8dtuHhVvJw9QYDQBjroK4aKyG9qqMD8cta
Pl/FAdyAqwH8Nw9efqAK+RQxSVUaue9BYEnbIRpsDK6Mkp3YMFmu5ki5AQoEUcxy
AAEIALyXYy8G2ZaTdJpdGcRhmIqOOSUlvP7/5E5BbYKBNu4KU3nX+JLvcF5jxPQ
42c7i/WRVxE1BJTiarKGsEvCi94TTXSIUKAt3T1oGBtXmGvqbGBqBjSGl1UTwdF
5yu5oJyRSf2fQrND6P/2eHNXejDUtdvhUXIU8h9MuUO/ipDoDnwIvMnAATJHA+R
Zqw6oNpyjRGzvr3iUWUwe4PtyJDI3ELAFkbp/NAC5TtUvHRHNOwnpldJhM5zHuB
QQb3G/EsCn2PQZ5w5SDzavF2SpvQfDqxYpDaTLAXtF+wsJL5iaUjxwRgJPodbCZf
2Tozd7h9MXtGJdIPKJ8eLG8ogcMAEQEAAYKBJQQYAQIADwUCUcxyAAIbDAUJCWYB
gAAKCRCTdsxl9/HZfs+hB/9BJqSmIgcoHFXnb1PVIKxekzL8+WVM5Pk/EgMQSLZ2
HX4p3ial5PEPEYgUw9YnaG4ioodwJGw5/dATWRrTzcnKd8YqoP+DUot96HZDSu3m
mCzE9NVAQYbFbVmGOXoeo627UBSvFqaXvAXBDYkoR8BoTnKhrQFwXkZVb3ohKwD
TgAFjOGIziE6uAdST231tFaqobizYfe5AVXRqro2oxBqNbaJNqs3SWoD83iSyvdv
lloBx83/Rogg7hUkI6F2vzXicWmUwFSXRggCSbLosHsP6isBWwvIHeRmna/aQab
YKG3gbV9jyczAS31gbogVLAZqNSWhp8vVIEE28Fyf/Ed
```

=x5FK

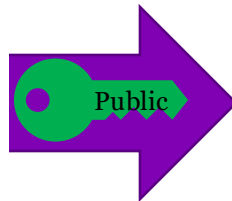
-----END PGP PUBLIC KEY BLOCK-----

Signature: 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



My public key



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

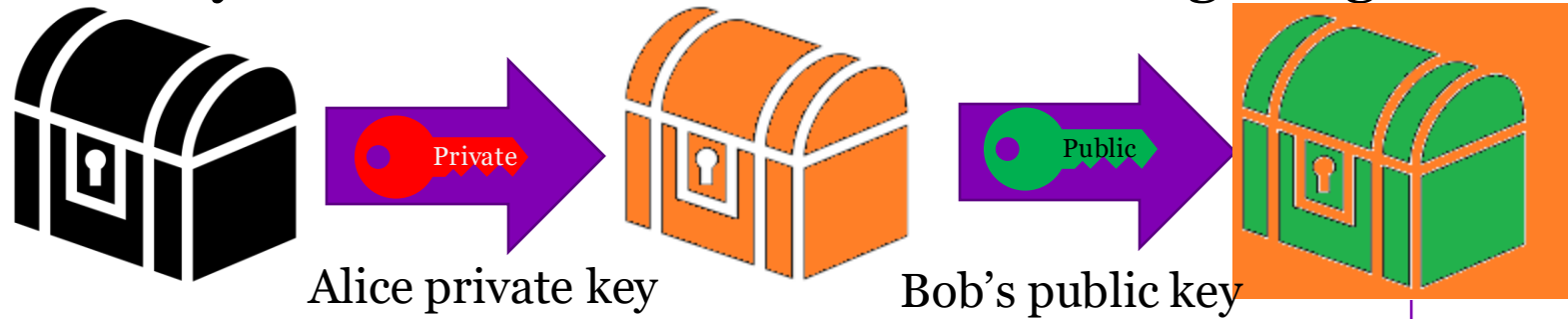
```
mQENBFHMcgABCAC9WrYDO6K2L3VHy14eHN6suHLqMpJ+SO+IUTuLEVNuzIoXAUXH
KozHejFV/9XoG8j933ZtszXKCog3aMESeoEoz6fNGfolvaCe5B4jwqoJt8NHw5L
B2dnqoCplgXcN2GJxfEHHUaf27COSobCJxPMeshU4ZHKke+g6DatmiEtBpVp41Ot
1zgxMqMkgb2H2xw28RYfykdDoueteIkOrFLrCy9ZF9KdMhA1eBH94Knw1QshdiZR
QYEX25+M8cKCb++Rc9H6an7EG9WHOFRW40UsY52OfveOyfQPzkkRto7u2339hvHo
B/h+7xLM6FQbOUZQ9BD5w7IQHgYtXJVsUjodABEBAAGOIktbWkgVmFuaWVhIDxr
dmFuaWVhQGluZi5lZC5hYy51az6JAT8EEwELACkFAIYKYvECGyMFCQlMAYAHcwkI
BwMCAQYVYCAIJCgsEFgIDAQIeAQIXgAAKCRCTdSxlg/HZffG+CACShuKxje3QAqew
GWh8K4gCdiYoxDqJwq3PHxmyhZmQeN/1a1KcOrIj12b+Q75/5t+EgXOHpRoPIxfG
LZ6zOEpf6A18fXx3JgQZdwPD0jtBiWNpOyMeBGTgIvEYg3so2VueQoeXcq3dbYp
5vstVxtD+TKHq5CioT75P2bzYq/XLT5aIbNqHqDPCTooDgbRH+FvqsRXr7yeaf
JaPnxXo+1L33t2QY9zctiGyebwrvHMrIPBJ2VYCDzQk7JuQ5eFh4ZhsMgOmzLQD4
YiGr5weIMFwAvxZOARxvEagVf48jiWvrXuJ8YfHWSohEScNOCYCp8q2oLJwwE26T
lpdtrwCqtBtLYW1pIFZhbmlYSA8a2FtaUB2YW5pZWUy9tPobkBgQTAQIALAlb
IwUJCWYBgAcLCQgHAWIBBhULAgKcQWAGMBAh4BAheABQJWCmMeAhkBAAoJEJN2
zGX38dl9JJAIAIWorxIYsrmKS6CbW8MgTxxTDOXA Ct1b7FoWoQZHskIUqhEcE+a
XBiyb1A5uHaatLfyjeXaD3qMEoZnQHoyMGEoGKUooWsbhfoQzHPgwzRLkDii75M
BtbawwoKWovB9e4AkMakXJCnF5BXeo6AHL2v15V205DikVnlCRXocKtu8b7LnmK
eLn7oLobr1de1uyKoNzbSnO/vpKDJPo/EY5yUeV9oIypZy/6wFQBehg1sXye6znO
9wb9uUs9+/P8pz4JILMDSevjfT7zSRSl/YP3fOfZ6N4bc+K0dwPM7u5Iyoeuqzh
pzibv3ge7VhH2xIWz8yVZ/2xT1345tWRRMOJAhwEEwECAAyFALTnSpEACgkQjyxM
p99tBt2B8A/+OpIzOsQbQJB8yxti4l7PpD1weJDF3a81Vhm7JyXE/Xy66ypfdt3w
XmFRUulrwezY1NebWNCRQHzQvRv/VJwjbTUX+Q3HsjIkKlHbE7CiQXxtTRkoEny
2nu dcjGI2voC3B2JCucEw6esF1x79PI/Pv2+6tgUBKmDfOpsB2vbtqrHnmAYKL
4lQBFH1YSJgnzwo2JkhhocHdF9oZem1eMeiDeeVkh63893N8Sww5fBKdJt+SKZ/L
rQElBBlpMR9BmeY6bPvWRuyvKkonIMR8oG9iFABxjTpWBL8aGk6EeVK5EqYDgVkd
ZlarK84r+KU1KD5IfgOCN7nhwgy7VI meE68caZHSRiPWZP1fVVMhydiRjv8WsoUs6
InFVU3nxH+ZYthPhYoT86leGSchBT5K/fBQvbjhrRTbTFwvjzSifb9efWylDi994
nzP6cNorir3GIpsT8gPGBB2/NjxaWiM6y3X1az1vRnsunQHuyKkFWPZwnEvDJYaC
NN/3jWcbhLFwKBDSaHps2+1meFPooJFvNetzp2bjT9a9pXaQ6KhOmo5DnhLcaV97
bFBpsUuBGaYZTSSo5x1RdXHqpEbgap8dtuHhVvJw9QYDQBjroK4aKyG9qqMD8cta
Pl/FAdyAqwH8Nw9efqAK+RQxSVUaue9BYEnbIRpsDK6MkP3YMFmu5ki5AQoEUcxy
AAEIALyXYy8G2ZaTdJpdGcRhmIqOOSUlpV7/5E5BbYKBNu4KU3nX+JLvcF5jxPQ
42c7i/WRVxE1BJTiarKGsEvCi94TTXSIUKAt3t1oGBtXmGvqbGBq8lJSGl1UTwdF
5yu5oJyRSf2qRND6P/2eHNXejDUtdvhUXIUth9MuUO/ipDoDnuwIvMnAATJHA+R
Zqw6oNpyjRGzvr3iUWUwe4PtyJDI3ELAFkbp/NAC5TtUvHRHNOwNpldJhM5zHuB
QQb3G/EsCn2PQZ5w5SDzavF2SpvQfDqxYpDaTLAXtF+wsJL5iaUjxwRgJPodbCZf
2Tozd7h9MXtGJdIPKJ8eLG8ogcMAEQEAAYKBJQQYAQIADwUCUcxyAAIbDAUJCWYB
gAAKCRCTdSxlg/HZfs+hB/9BJqSmIgcoHFXnb1PVIKxekzL8+WVM5Pk/EgMQSLZ2
HX4p3ial5PEPcYgUw9YnaG4ioodwJGw5/d4TWRrTznKd8YqoP+DUot96HZDSu3m
mCzE9NVAQYboFbVmGOxoeo627UBSvFqaXvAXBDYkoR8BoTnKhrQFwXkZVb3ohKwD
TgAFjOGIziE6uAdST231tFaqobizYfe5AVXRqro2oxBqNbaJNqs3SWoD83iSyv dv
lloBx83/Rogg7hUkI6F2vzXicWmUwFSXRggCSbLosHsP6isBWwvlHeRmna/aQab
YKG3gbV9jyczAS31gbogVLAZqNSWhp8vVIEE28Fyf/Ed
```

=x5FK

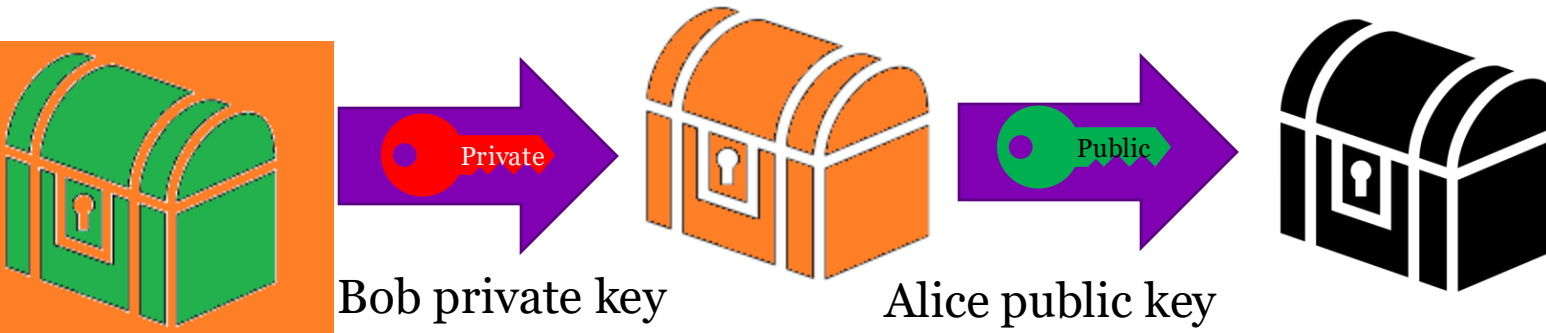
-----END PGP PUBLIC KEY BLOCK-----

If Alice does both of those at the same time she can prove that:

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



2. only Bob can read it (encryption)



- Signature:
 k_{PRIV} can encrypt and k_{PUB} can decrypt

$$P = D(k_{\text{PUB}}, E(k_{\text{PRIV}}, P))$$

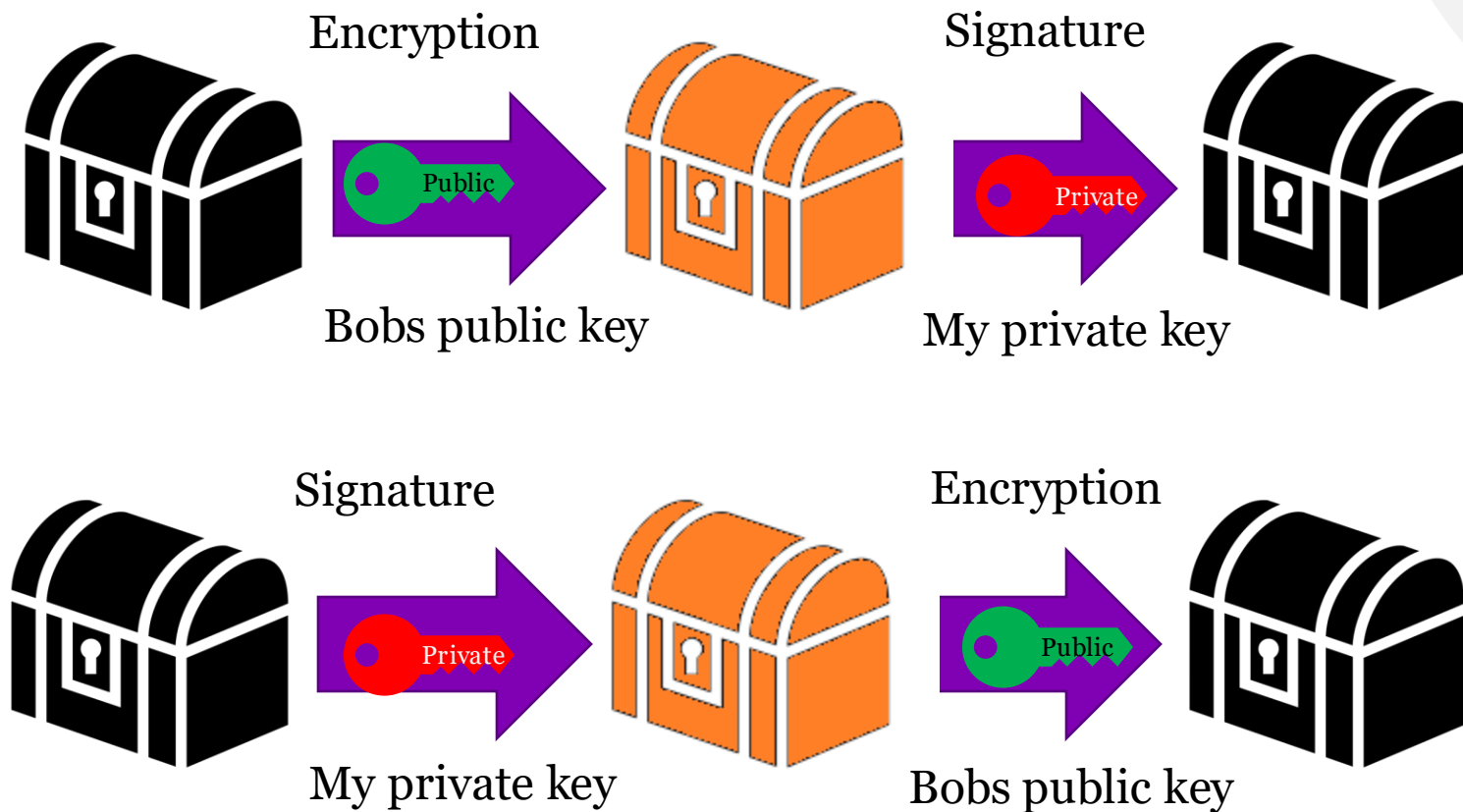
- Encryption:
 k_{PUB} can encrypt and k_{PRIV} can decrypt

$$P = D(k_{\text{PRIV}}, E(k_{\text{PUB}}, P))$$

- Signing and encrypting:
 $P = D(A_{\text{PUB}}, D(B_{\text{PRIV}}, E(B_{\text{PUB}}, E(A_{\text{PRIV}}, P))))$

Think-pair-share

- When both encrypting and signing a message. The order of encryption and signature matters. What attack is possible if the order is reversed?



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

ASYMMETRIC KEY GENERATION

Knapsack problem

Given a set of items, each with a weight and a value, determine which items to include in the collection so that the total weight is less than or equal to a given limit and the total value is as large as possible.

Knapsack cryptosystem

- Not secure by modern systems, but much easier to understand than RSA
- Based on the NP hard Knapsack problem: given a set of weights of items find the set of items that equal an exact weight
- Easy to solve for superincreasing knapsacks where each weight is $>$ the sum of all prior weights
- Example: $\{3, 6, 11, 25, 46, 95, 200, 411\}$

Given a set of n weights
 $W = (W_0, W_1, \dots, W_{n-1})$

and a desired sum S ,

find $(a_0, a_1, \dots, a_{n-1})$ where $a_i \in \{0, 1\}$

Such that

$$S = a_0 W_0 + a_1 W_1 + \dots + a_{n-1} W_{n-1}$$

Knapsack cryptosystem

1. Select a superincreasing knapsack
 $\{2, 3, 7, 14, 30, 57, 120, 251\}$ – private key
2. Convert to general-looking knapsack using a selected multiplier (41) and modulus (491)
 - Resulting generic knapsack is NP hard to solve
 - $\{82, 123, 287, 83, 248, 373, 10, 471\}$ – public key
3. Compute the multiplicative inverse of the conversion factor, i.e. $m^{-1} \bmod n$
 - $12 = (2, 3, 7, 14, 30, 57, 120, 251)$ and $41^{-1} \pmod{491}$

Conversion to generic knapsack

Computation	Generic Knapsack
$2 * 41 \bmod 491$	82
$3 * 41 \bmod 491$	123
$7 * 41 \bmod 491$	287
$14 * 41 \bmod 491$	83
$30 * 41 \bmod 491$	248
$57 * 41 \bmod 491$	373
$120 * 41 \bmod 491$	10
$251 * 41 \bmod 491$	471

Knapsack: Alice wants to encrypt for Bob

- $M = 10010110$
- Bob's public key:
 $\{82, 123, 287, 83, 248, 373, 10, 471\}$
- Use Bob's public key to select values

K_{pub}	82	123	287	83	248	373	10	471
M	1	0	0	1	0	1	1	0
C	82			83		373	10	

- Add values:
 $548 = 82 + 83 + 373 + 10$
- Alice sends 548

- Bob computes:
 $m^{-1} \cdot C \pmod{n} = 12 \cdot 548 \pmod{491} = 193$
- Bob uses his private key to compute 193

K_{priv}	2	3	7	14	30	57	120	251
M								

Try and work out what
should be in the plaintext
(message) row

Knapsack: Alice wants to encrypt for Bob

- $M = 10010110$
- Bob's public key:
 $\{82, 123, 287, 83, 248, 373, 10, 471\}$
- Use Bob's public key to select values

K_{pub}	82	123	287	83	248	373	10	471
M	1	0	0	1	0	1	1	0
C	82			83		373	10	

- Add values:
 $548 = 82 + 83 + 373 + 10$
- Alice sends 548

- Bob computes:
 $m^{-1} \cdot C \pmod{n} = 12 \cdot 548 \pmod{491} = 193$
- Bob uses his private key to compute 193

K_{priv}	2	3	7	14	30	57	120	251
M	1	0	0	1	0	1	1	0

Knapsack cryptosystem

- Not secure by modern systems, but much easier to understand than RSA
- Knapsack is NP hard, which makes it a sorta ok cryptosystem even today. But it can be broken.



Elfenland Board Game – Basically the traveling salesman problem. Even NP hard problems can be easy/fun at small scale.

RSA – Rivest, Shamir, and Adleman (the inventors)

- Modern standard used by many products
- Unlike Knapsack it is based on prime factorization, which is not proven to be NP complete
- RSA security rests on prime factorization being a hard problem



Adi Shamir, co-inventor of RSA

Photo credit: Ira Abramov from Even Yehuda, Israel -
<https://www.flickr.com/photos/38872520@N00/3814143223/>

RSA – Rivest, Shamir, and Adleman (the inventors)

- To generate, chose two large prime numbers p and q and form their product
 - $N = pq$
- Choose e relatively prime to the product
 - $d = (p-1)(q-1)$
- Public key: (N, e)
Private key: d
- Compute the cypher C of message M
 - $C = M^e \bmod N$
- Decrypt C
 - $M = C^d \bmod N$
- This works if we assume:
 - $M = C^d \bmod N = M^{ed} \bmod N$

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.

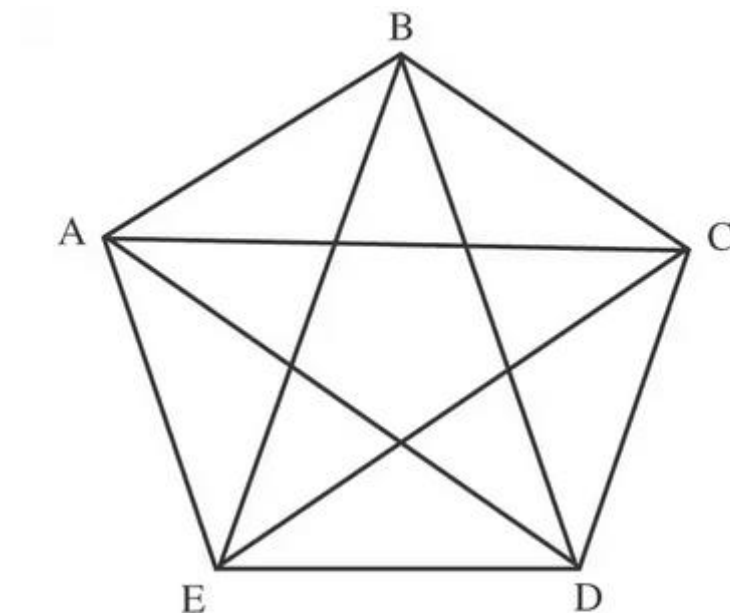
How do we solve the identity problem?

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

Approach scales poorly

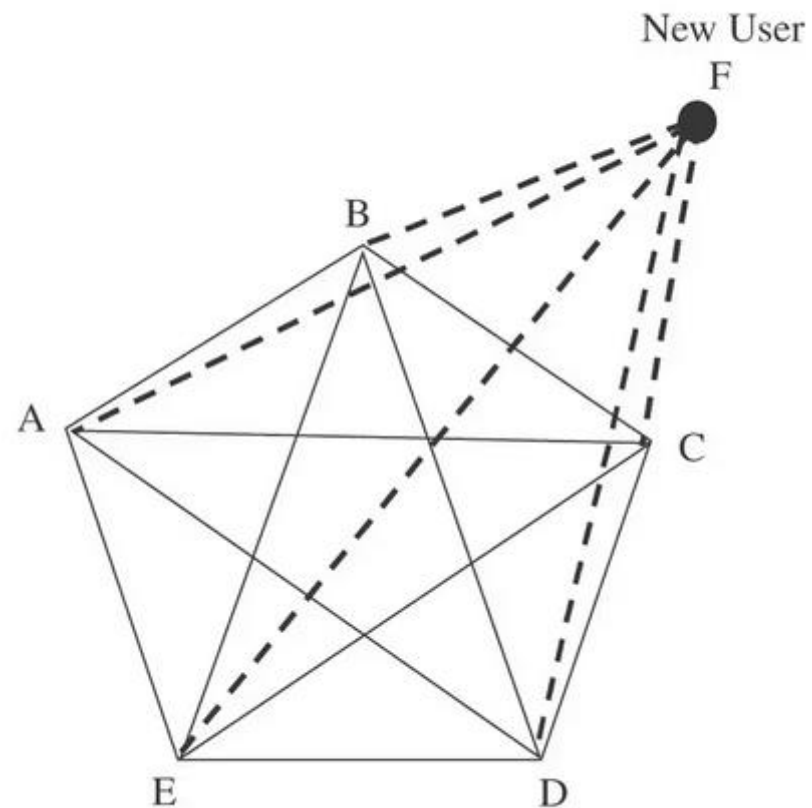
An n user system requires $n*(n-1)/2$ keys

Expecting people to verify that many keys, as well as store and not lose them is unreasonable



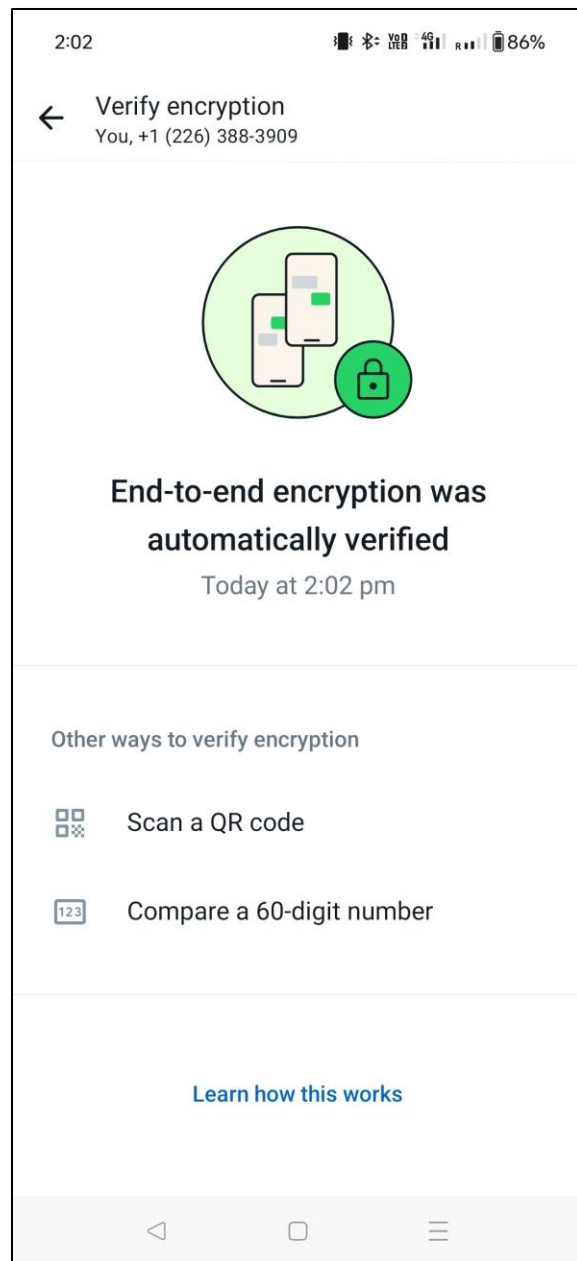
Existing Users

New Keys to Be Added - - - - -

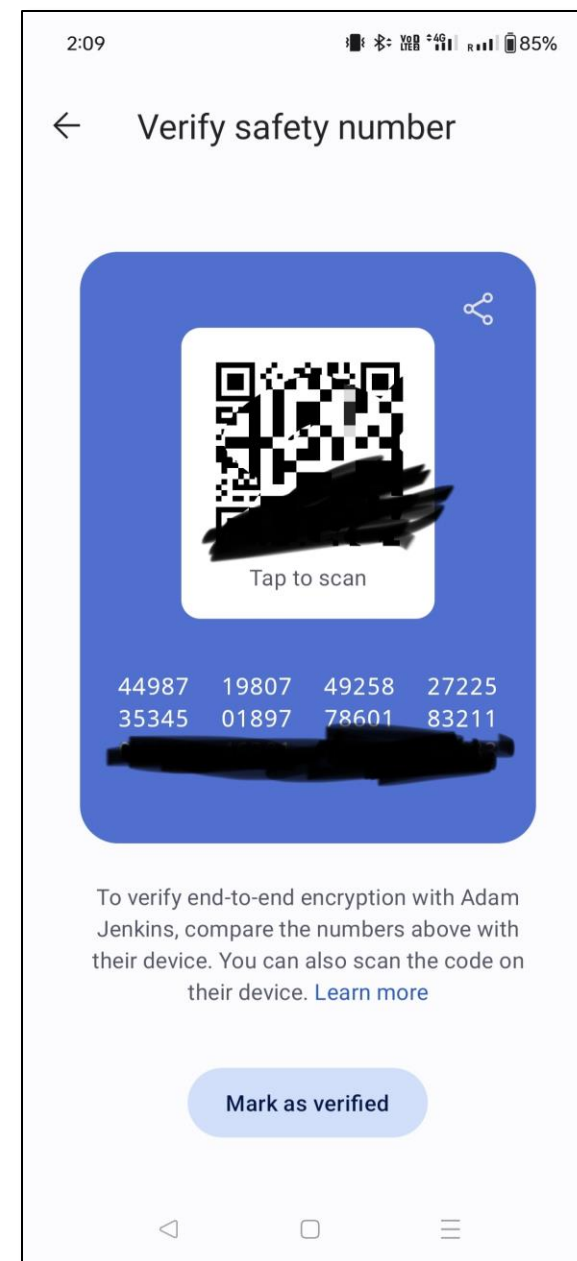


User comparing of keys is still used for verification today by common apps like WhatsApp and Signal.

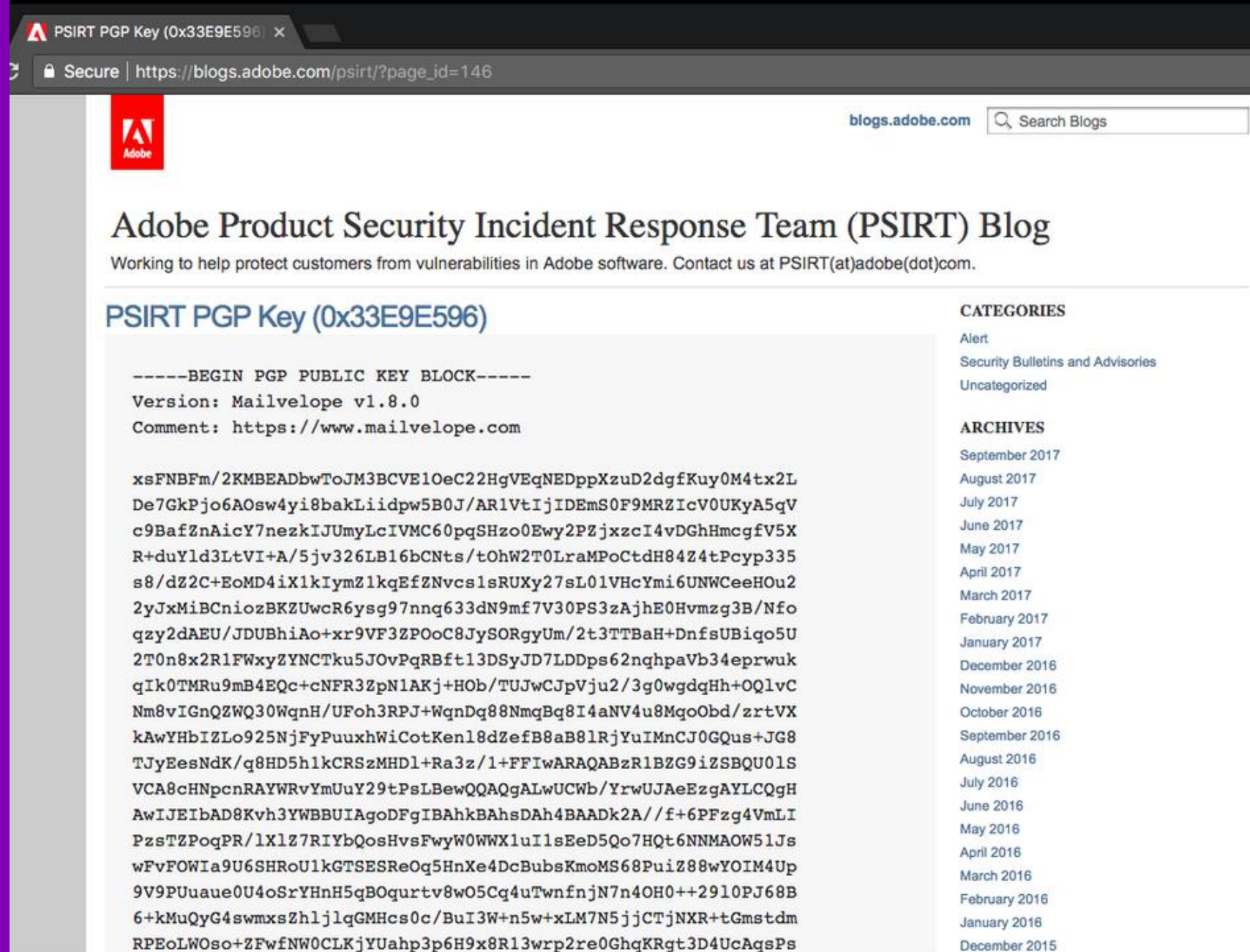
WhatsApp



Signal



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



The screenshot shows a web browser window with the Adobe PSIRT Blog. The page title is "PSIRT PGP Key (0x33E9E596)". The main content area displays a PGP public key block. The key block starts with "-----BEGIN PGP PUBLIC KEY BLOCK-----" and ends with "-----". The key is for "Mailvelope v1.8.0" and the comment is "https://www.mailvelope.com". The key data is a long string of characters. The right sidebar contains "CATEGORIES" (Alert, Security Bulletins and Advisories, Uncategorized) and "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).

PSIRT PGP Key (0x33E9E596)

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

xsFNBfM/2KMBEADbwToJM3BCVE1OeC22HgVEqNEDppXzuD2dgfKuy0M4tx2L
De7GkPjo6AOsw4yi8bakLiidpw5B0J/ARlVtIjIDeMS0F9MRZicV0UKyA5qV
c9BafZnAicY7nezkJUmyLcIVMC60pgSHzo0Ewy2PZjxzcI4vDGhHmcgfv5X
R+duYld3LtVI+A/5jv326LB16bCNts/tOhW2T0LraMPOctdH84Z4tPcyp335
s8/dZ2C+EoMD4iX1kIymZ1kqEfZNvcs1sRUXy27sL01VHcYmi6UNWCeeHOu2
2yJxMiBCniozBKZUwcR6ysg97nnq633dN9mf7V30PS3zAjhE0Hvmzg3B/Nfo
qzy2dAEU/JDUBhiAo+xr9VF3ZPOoC8JySORgyUm/2t3TTBaH+DnfsUBiqo5U
2T0n8x2R1FWxyZYNCTku5JOvPqRBft13DSyJD7LDDps62nqhpavb34eprwuk
qIk0TMRu9mB4EQc+cNFR3ZpN1AKj+HOb/TUJwCJpVju2/3g0wgdqHh+OQlvC
Nm8vIGnQZWQ30WqnH/UFoh3RPJ+WqnDq88NmQBg8I4aNV4u8MgoObd/zrtVX
kAwYHbIZLo925NjFyPuuxhWiCotKenl8dZefB8aB81RjYuIMnJCJ0GQus+JG8
TJyEesNdK/q8HD5h1kCRSzMHD1+Ra3z/1+FFIwARAQABzR1BZG9iZSBQU01S
VCA8cHNpcnRAYWRvYmUuY29tPsLBewQQAQgALwUCWb/YrWUJAEZgAYLCQGH
AwIJEIbAD8Kvh3YWBBUIAgoDFgIBAhkBAhsDAH4BAADk2A//f+6PFzg4VmLI
PzstZPoqPR/lXlZ7RIYbQosHvsFwyW0WWXluIlsEeD5Qo7HQt6NNMAOW51Js
wFvFOWIa9U6SHRoU1kGTSESReOq5HnXe4DcBubsKmoMS68PuiZ88wYOIM4Up
9V9PUuaue0U4oSrYHnH5qBOqurtv8wO5Cq4uTwnfnjN7n4OH0++2910PJ68B
6+kMuQyG4swmxsZhljlqGMHcs0c/BuI3W+n5w+xLM7N5jjCTjNXR+tGmstdm
RPEoLW0so+ZFwfNW0CLKjYUahp3p6H9x8R13wpr2re0GhqKRGt3D4UcAqsPs

Photo credit: Juho Nurminen
@jupenur

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

```
xsFNBfM/2KMBEADbwToJM3BCVE1OeC22HgVEqNEDppXzuD2dgfKuy0M4tx2L
De7GkPjo6AOsw4yi8bakLiidpw5B0J/AR1VtIjIDeMS0F9MRZicV0UKyA5qV
c9BafZnAicY7nezkiJUmYLCiVMC60pqSHzo0Ewy2PZjxzcI4vDGhHmcgfV5X
R+duYld3LtVI+A/5jv326LB16bCNts/tOhW2T0LraMPoCtdH84Z4tPcyp335
s8/dZ2C+EOmd4iX1kIymZ1kqEfZNvcs1sRUXy27sL01VHcYmi6UNWCeeHOu2
2yJxMiBCniozBKZUwcr6ysg97nnq633dN9mf7V30PS3zAjhE0Hvmzg3B/Nfo
qzy2dAEU/JDUBhiAo+xr9VF3ZPOoC8JySORgyUm/2t3TTBaH+DnfsUBiqo5U
2T0n8x2R1FWxyZYNCtku5JOvPqRBft13DSyJD7LDDps62nqhpaVb34eprwuk
qIk0TMRu9mB4EQc+cNFR3ZpN1AKj+HOb/TUJwCJpVju2/3g0wgdqHh+OQlvC
Nm8vIGnQZwQ30WqnH/UFoh3RPJ+WqnDq88NmQBq8I4aNV4u8MgoObd/zrtVX
kAwYHbIZLo925NjFyPuuxhWiCotKenl8dZefB8aB81RjYuIMnJCJ0GQus+JG8
TJyEesNdK/q8HD5h1kCRSzMHD1+Ra3z/1+FFIwARAQABzR1BZG9iZSBQU01S
VCA8cHNpcnRAYWRvYmUuY29tPSLBewQQAQgALwUCWb/YrWUJAEZgAYLCQgH
AwIJEIbAD8Kvh3YWBbUIAgoDFgIBAhkBAhsDAH4BAADk2A//f+6PFzg4VmLI
PzsTZPoqPR/lXlZ7RIYbQosHvsFwyW0WWX1uIlsEeD5Qo7HQ6NNMAOW51Js
wFvFOWIa9U6SHRoU1kGTSESReOq5HnXe4DcBubsKmoMS68PuiZ88wYOIM4Up
9V9PUuaue0U4oSrYHnH5qBOqurtv8wO5Cq4uTwnfnjN7n4OH0++2910PJ68B
6+kMuQyG4swmxsZhlj1qGMHcs0c/BuI3W+n5w+xLM7N5jjCTjNXR+tGmstdm
RPEoLW0so+ZFwfNW0CLjYUahp3p6H9x8R13wrp2re0GhqKRgt3D4UCaQsPs
```

Photo credit: Juho Nurminen
@jupenur

PSIRT PGP Key (0x33E9E596) x

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

blogs.adobe.com

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
c9BafZnAicY7nezkiJUmYLCiVMC60pqSHzo0Ewy2PZjxzcI4vDGhHmcgfV5X
R+duYld3LtVI+A/5jv326LB16bCNts/tOhW2T0LraMPoCtdH84Z4tPcyp335
s8/dZ2C+EOmd4iX1kIymZ1kqEfZNvcs1sRUXy27sL01VHcYmi6UNWCeeHOu2
2yJxMiBCniozBKZUwcr6ysg97nnq633dN9mf7V30PS3zAjhE0Hvmzg3B/Nfo
qzy2dAEU/JDUBhiAo+xr9VF3ZPOoC8JySORgyUm/2t3TTBaH+DnfsUBiqo5U
2T0n8x2R1FWxyZYNCtku5JOvPqRBft13DSyJD7LDDps62nqhpaVb34eprwuk
qIk0TMRu9mB4EQc+cNFR3ZpN1AKj+HOb/TUJwCJpVju2/3g0wgdqHh+OQlvC
Nm8vIGnQZwQ30WqnH/UFoh3RPJ+WqnDq88NmQBq8I4aNV4u8MgoObd/zrtVX
kAwYHbIZLo925NjFyPuuxhWiCotKenl8dZefB8aB81RjYuIMnJCJ0GQus+JG8
TJyEesNdK/q8HD5h1kCRSzMHD1+Ra3z/1+FFIwARAQABzR1BZG9iZSBQU01S
VCA8cHNpcnRAYWRvYmUuY29tPSLBewQQAQgALwUCWb/YrWUJAEZgAYLCQgH
AwIJEIbAD8Kvh3YWBbUIAgoDFgIBAhkBAhsDAH4BAADk2A//f+6PFzg4VmLI
PzsTZPoqPR/lXlZ7RIYbQosHvsFwyW0WWX1uIlsEeD5Qo7HQ6NNMAOW51Js
wFvFOWIa9U6SHRoU1kGTSESReOq5HnXe4DcBubsKmoMS68PuiZ88wYOIM4Up
9V9PUuaue0U4oSrYHnH5qBOqurtv8wO5Cq4uTwnfnjN7n4OH0++2910PJ68B
6+kMuQyG4swmxsZhlj1qGMHcs0c/BuI3W+n5w+xLM7N5jjCTjNXR+tGmstdm
RPEoLW0so+ZFwfNW0CLjYUahp3p6H9x8R13wrp2re0GhqKRgt3D4UCaQsPs
```

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

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

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
GAElABkFAlm/2LAFCQHhM4AJElbAD8Kvh3YWAhsMAACz+g/+KmbnChEUZXdo
ZIVpZphw3KvZQHWCY+5qGqdoxNkfkUSKhkzC0M51Kq7emVpVXYrMRdJRHxFP
83HIahA5UiufsDt7QlMwVRgtJYxhH+TNZBBbDBVQlJQXuC3mH7F/tFhb9N1G
kURUwa2fdDBPw2+DOWa2+iVhcPhfB2iy9exs2txXjgPx67aZi70Jw44ixvpY
TWs/M5I6SXQsyuB5Qw0jtXKioQyTOLmeUFmJR2Ui5FK+t5SXus44mRCuJEUn
YDqDmxKDNhssEVNWZ4KWs2uvNXNwlnZcHVSyXukf3F1CWp0TESCOecdqbv10
Cs+vLivixksh33xqZWnD78xv92t2Ggp2a41gBOaaCjx2irqZ9RHiv0YzNfQz
yz5XYEGI2iCrvdStrbZfX1Dqsllrqs/pZRbV48KbubDvGZuNR3hrsfmfsgr
zkESOQmpuKhj/Es3CKjdafLDc8H0yVhJ+n4tvWXyRpyEhuDh/tzeDuuB9vfG
QA9TNhSpAp5lHFJklmd9knWbExJ0srUbK2QVnVn9CZx/sdUfwDWp1GeANLsO
MRNlr3Irk1bZ0bFH+nrcJQZ5+sDzHGNe4P9Dt30yvFHOyS1BkRndLuawSlqh
LJyYLUvFjL3i3jbiNT1NKldwqaL2i9OuRAuHthoFGOKIqr6hmtOYzUem/cl+
ZlRwd77Vmfc=
=QOc7
```

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

-----BEGIN PGP PRIVATE KEY BLOCK-----

Version: Mailvelope v1.8.0

Comment: <https://www.mailvelope.com>

```
xcaGBFm/2KMBEADbwToJM3BCVE1OeC22HgVEqNEDppXzuD2dgfKuy0M4tx2L
De7GkPjo6AOsw4yi8bakLiidpw5B0J/AR1VtIjIDeMS0F9MRZICv0UKyA5qV
c9BafZnAicY7nezkiJUmYlCIVMC60pqSHzo0Ewy2PZjxzcI4vDGhHmcgfV5X
R+duYld3LtVI+A/5jv326LB16bCNTs/tOhW2T0LraMPoCtdH84Z4tPcyp335
s8/dZ2C+EoMD4iX1kIymZ1kqEfZNvcs1sRUXy27sL01VHcYmi6UNWCeeHOu2
2yJxMiBCniozBKZUwcR6ysg97nnq633dN9mf7V30PS3zAjhe0Hvmzg3B/Nfo
qzy2dAEU/JDUBhiAo+xr9VF3ZPOoC8JySORgyUm/2t3TTBaH+DnfsUBiqo5U
2T0n8x2R1FWxyZYNCTku5JOvPqRBft13DSyJD7LDDps62nqhpaVb34eprwuk
qIk0TMRu9mB4EQc+cNFR3ZpN1AKj+HOb/TUJwCJpVju2/3g0wgdqHh+OQlvC
Nm8vIGnQZWQ30WqnH/UFoh3RPJ+WqnDq88NmQBq8I4aNV4u8MqoObd/zrtVX
kAwYHbIZLo925NjFyPuuxhWiCotKenl8dZefB8aB81RjYuIMnCJ0GQus+JG8
TJyEesNdK/q8HD5h1kCRSzMHD1+Ra3z/1+FFIwARAQAB/gkDCA7HXpjNu7yW
YBVIglTandp2qwxLZTA0Jm3YMOwvBojE4ZDL41VZBh2sBphQ15CLulx7MUrD
```

Do not do this

April 2014
March 2014
February 2014
January 2014
December 2013
November 2013
October 2013
September 2013
July 2013
June 2013
May 2013
April 2013
March 2013
February 2013
January 2013
December 2012
November 2012
October 2012
September 2012
August 2012
July 2012
June 2012
May 2012
April 2012
March 2012
February 2012
January 2012
December 2011
November 2011
October 2011
September 2011
August 2011
July 2011
June 2011
May 2011
April 2011
March 2011
February 2011
December 2010

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).
- Key signing parties 

My public key

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

```
mQENBFHMcgABCAC9WrYDO6K2L3VHy14eHN6suHLqMpJ+SO+IUTuLEVnUzIoXAUXH
KozHejV/9XoG8j933ZtszXKCog3aMESeoEoz6fNGfolvaCe5B4jwqoJt8NHw5L
B2dnqoCplgXcN2GJxfEHHUaf27COSobCjXpMeshU4ZHKke+g6DatmiEtBpVp41Ot
1zxdmMQkgb2H2xw28RYfykdDoueteIkOrFLrCy9ZF9KdMhA1eBH94Knw1QshdiZR
QYEX25+M8cKCb++Rc9H6an7EG9WHOFRW40UsY52OfveOyfQPzkkRto7u2339hvHo
B/h+7xLM6FQbOUZQ9BD5w7IQHgYtXJV5UjodABEBAAgoIkthbWkgVmFuaWVhIDxr
dmFuaWVhQGluZi5lZC5hYy51az6JAT8EEwELACkFAlYKYvECGyMFCQlmAYAHcwkI
BwMCAQYVCAIJCgsEFgIDAQIeAQIXgAAKCRCTdSxlg/HZffG+CACShuKxje3QAqew
GWh8K4gCdiYoxDqJwq3PHxmyhZmQeN/1a1KcOrIj12b+Q75/5t+EgXOHpRoPIxfG
lZ6zOEpf6A18iFXx3JgQZdwPD0jtBiWNpOyMeBGTgIvEYg3so2VueQoeXcq3dbYp
5vstVxtD+TKHQ5CioT75P2bzYq/XLT5aIbNQHqDPcToDgBRH+FvqsRXr7yeaef
JaPnxXo+1L33t2QY9zctiGyebwrtVHMrIPBJ2VYCDzQk7JuQ5eFh4ZhsMgOmzLQD4
YiGr5weIMFwAvxZOaRxEa9Vf48jiWvrxuJ8YfHWSohEScNOCYCzP8q2olwwE26T
lpdtrwCqtB1LYW1pIFZhbmllySA8a2FtaUB2YW5pZWEuY29tPokBQgQTAQIALiAb
IwUJCWYBgAcLCQgHAWIBBHULAgkKCwQWAgMBAh4BAheABQJWCmMeAhkBAAoJEJN2
zGX38dl9JJAIAIWorxrlYsrmKS6CbW8MgTxxTDOXA Ct1b7FoWoQZHsklUQhEcE+a
XBiyib1A5uHaatLfyjeXaD3qMEoZnQHoyMGEoGKuooWsbhfoQzHPgwzRLkDii75M
B1bawwoKWoVB9e4AkMakXJCnF5BXeo6AHLRL2v15V205DikVnlCRXocKtu8b7LnmK
eLn70Lobr1de1uyKoNzbSnO/vpKDJPo/EY5yUeV9oIypZy/6wFQBehg1sXye6znO
9wb9uUsug+/P8pz4JILMDSevjfT7zSRSL/YP3fOfZ6N4bc+K0dwPM7u5Iyoeu9zh
pzibv3ge7VhH2xIWz8vYZ/2xT1345tWRRMOJAhwEEwECAAyFALTnSpEACgkQjyxM
p99tBt2B8A/+OpIzOsQbQJB8yxti4l7PpD1weJDF3a81Vhm7JyXE/Xy66ypfdt3w
XmFRUuIrwezY1NebWNCRQHHzQvRv/VJwbjTUX+Q3HsjIkKlHbE7CiQXXtTRkoEny
2nuGjGI2vo3C3B2JCucEw6esF1x79Pl/Pv2+6tgUBKmDfOpsB2vbtqrHnmAYKL
4lQBFH1YSJgnzwo2JkhhocHdF9oZem1eMeiDeeVkh63893N8Swk5fBKdTj+SKZ/L
rQElBBlpMR9BmeY6bPvWRuyvKkonIMR8oG9iFABxjTpWBL8aGk6EeVK5EqYDgVkd
ZlarK84r+KU1KD5lfgOCN7nhwgy7VI me68caZHSRiPWZP1fVVMhydiRjv8WsoUs6
InfVU3nxH+ZYthPbYoT86leGSchBT5K/fbQvbjhrRTbTfwvjzSifb9efWylDi994
nzP6cNorir3GIpsT8gPgBB2/NjxaWiM6y3X1az1vRnsunQHuyKkFWPZwnEvDJYaC
NN/3jUwcbhLFwKBDsaHps2+1meFPooJFvNetzpbjT9a9pXaQ6KhOmo5DnhLcaV97
bFBpsuUBGaYZTSSo5x1RdXHqpEbgap8dtuHhVvJw9QYDQBjroK4aKyG9qqMD8cta
Pl/FAdyAqWH8Nw9efqAK+RQxSVUaue9BYEnbIRpsDK6MkP3YMFmu5ki5AQoEUcxy
AAEIALyXYy8G2ZaTDJpdGcRhmIqOOSUlzPV7/5E5BbYKBNu4KU3nX+JLvcF5jxPQ
42c7i/WRVxE1BJTiarKGsEvCi94TTXSIUKAt3T1oGBTxmGvqbGBq8ljSGl1UTwdF
5yu5oJyRSf2fqRND6P/2eHNXeJDUTdvhUXIUt8h9MnAUO/ipDoDnwIvMnAATJHA+R
Zqw6oNpyjRGzvr3iuWUwe4PtyJDI3ELAFkbp/NAc5TiuVHRHNOwnpldJhM5zHuB
QQb3G/EsCn2PQZ5w5SDzavF2SpvQfDqxYpDaTLAXtF+wsJL5iaUjxwRgJPodbCZf
2Tozd7h9MXtGJDlPKJ8eLG8ogcMAEQEAAYkBJQQYAQIADwUCUcxyAAIbDAUJCWYB
gAAKCRCTdSxlg/HZfS+hB/9BJqSmIgcoHFXnb1PVIKxekzL8+WVm5Pk/EgMQSLZ2
HX4p3ial5PEPEYgUw9YnaG4ioodwJGw5/daTWRRtZcnKd8YqoP+DUOt96HZDSu3m
mCzE9NVAQYboFbVmGOxoeo627UBSvFqaXvAxBDYkoR8BoTnKhrQFwXkZVb3ohKwD
TgAFjOGIziE6uAdST231tFaqobizYfe5AVXRqro2oxBqNbaJNqs3SWoD83iSyvdv
lIOBx83/Rogg7hUkI6F2vzXicWmUwFSXRggCSbLosHsP6isBWwvlHeRmna/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

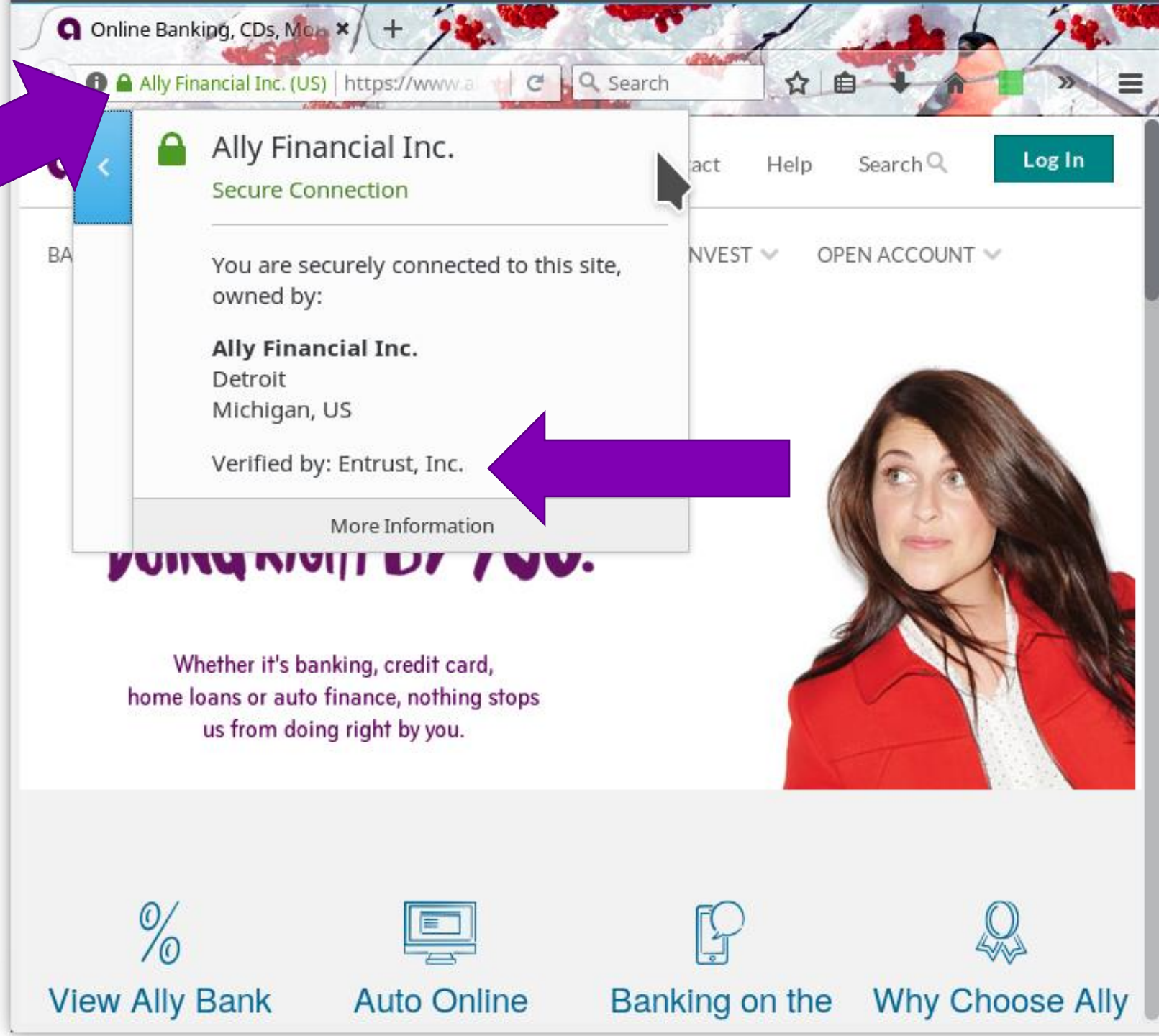
Field Value

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**



You can see
lots of details
about any
encrypted
connection.

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

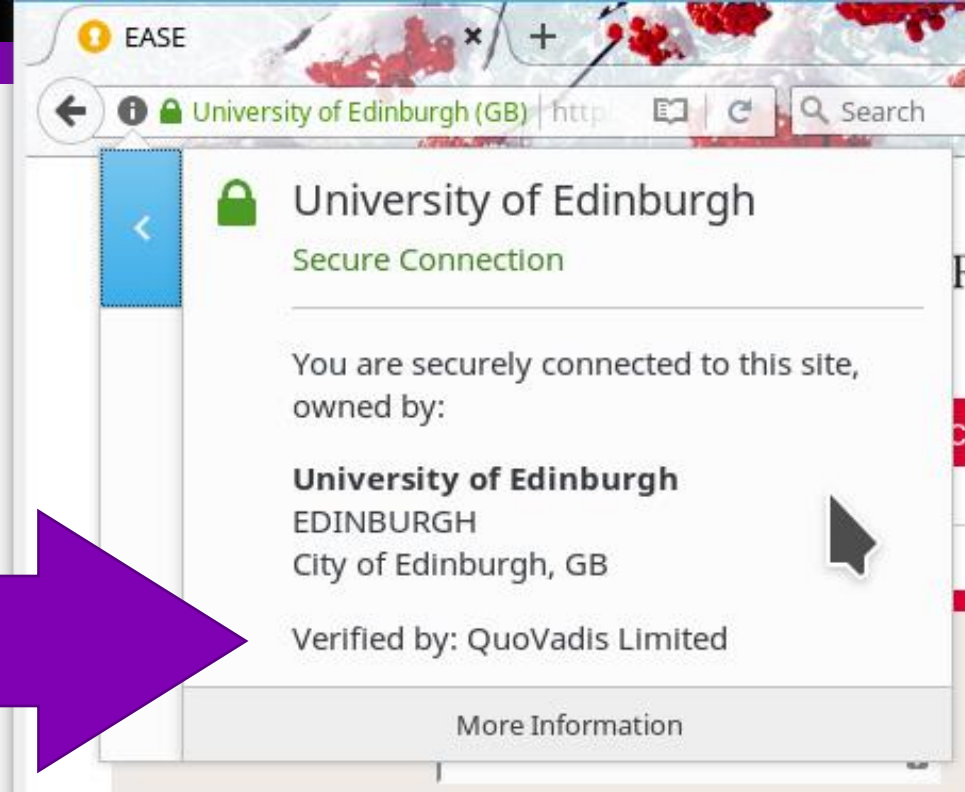
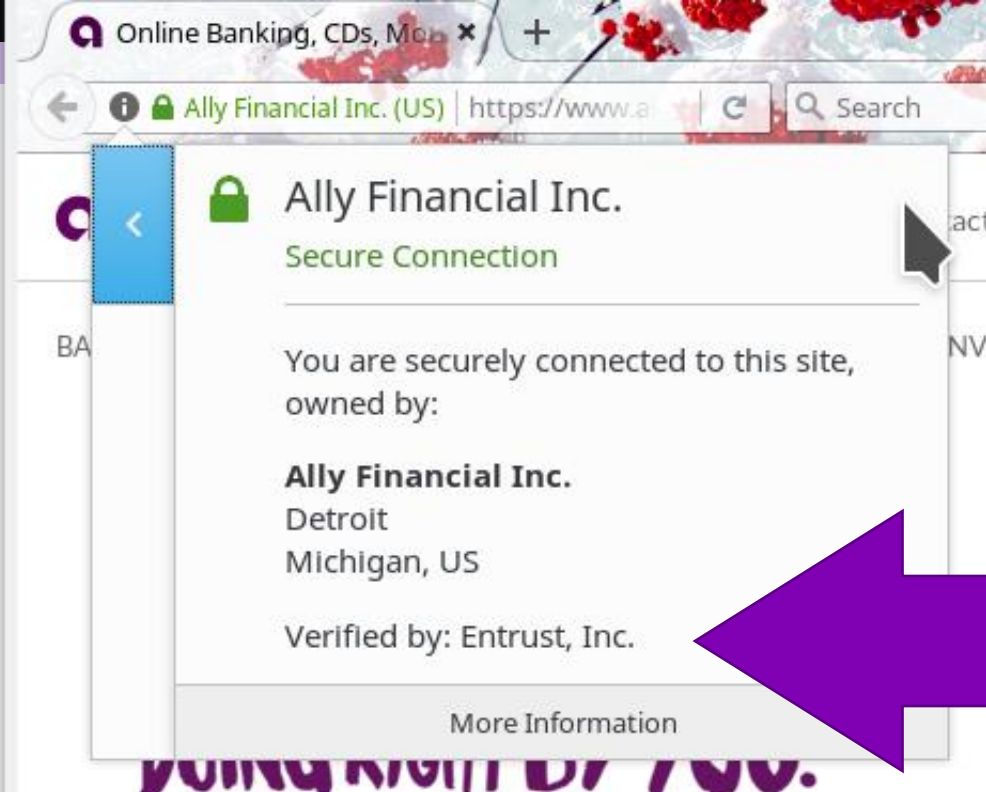
Technical Details

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.

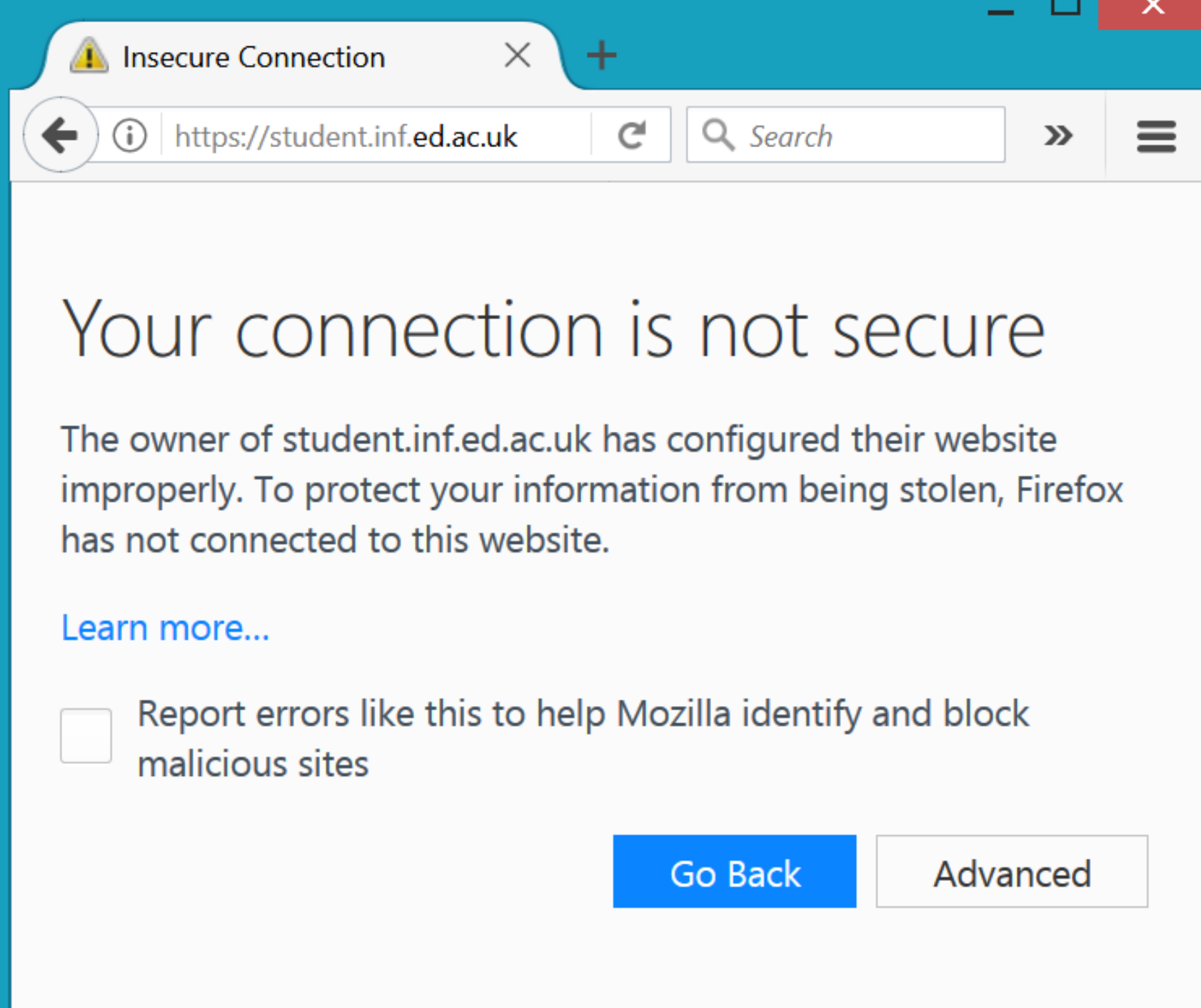
Encryption makes it difficult for unauthorised people to view information travelling between computers. It is therefore unlikely that anyone read this page as it travelled across the network.

[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.**



Errors on
student.inf.ed.ac.uk
are a bit easier to
understand though,
identity information
is missing...

Page Info - https://student.inf.ed.ac.uk/

General Media Security

Web Site Identity

Web site: student.inf.ed.ac.uk

Owner: **This web site does not supply ownership information.**

Verified by: **Not specified**

Privacy & History

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

Technical Details

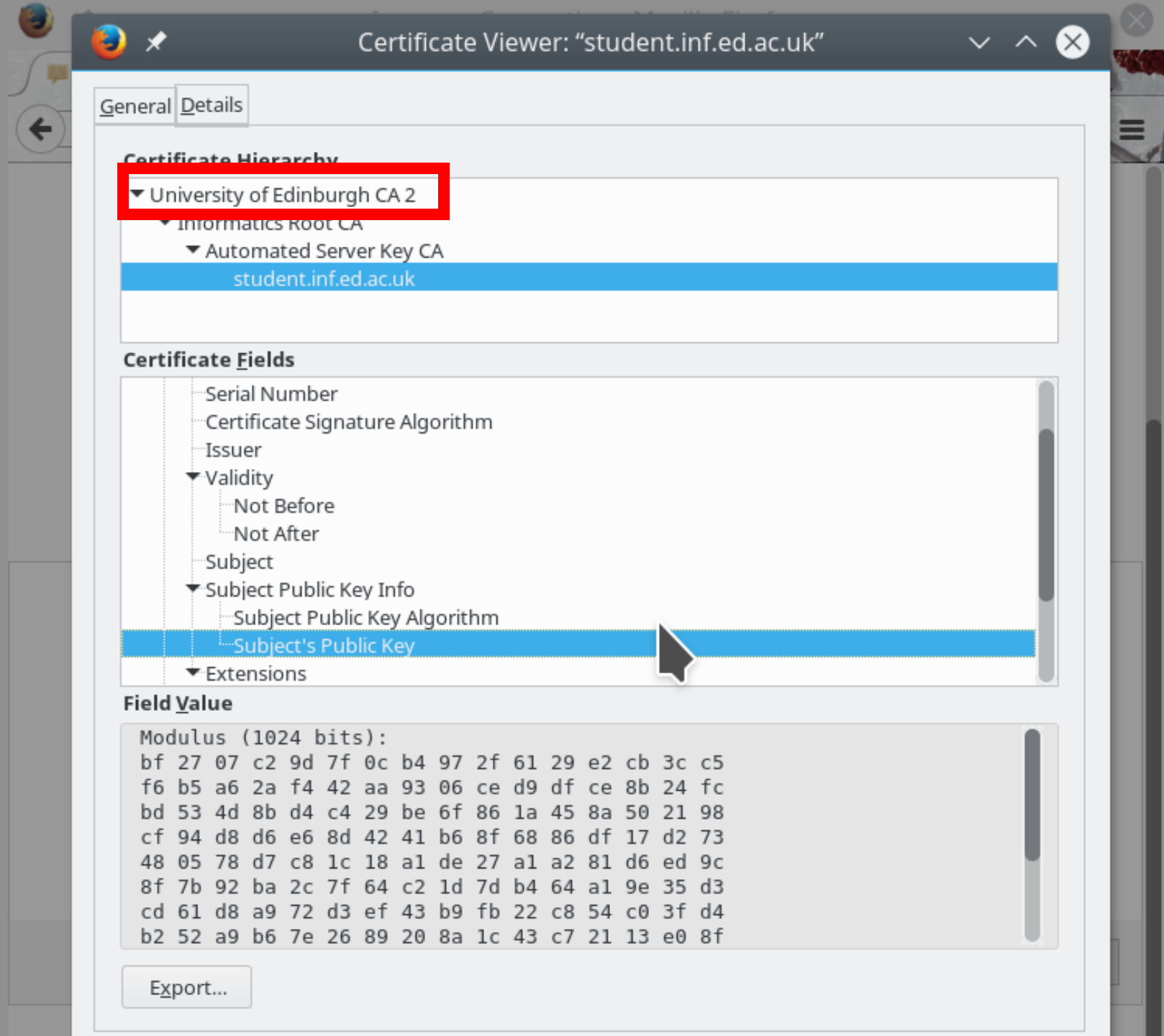
Connection Not Encrypted

The web site student.inf.ed.ac.uk does not support encryption for the page you are viewing. Information sent over the Internet without encryption can be seen by other people while it is in transit.

[Help](#)

This site is “self signed” which means that the University created its own Certificate Authority and used it to sign all the sites keys.

Why? It costs money to get a signed certificate.



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

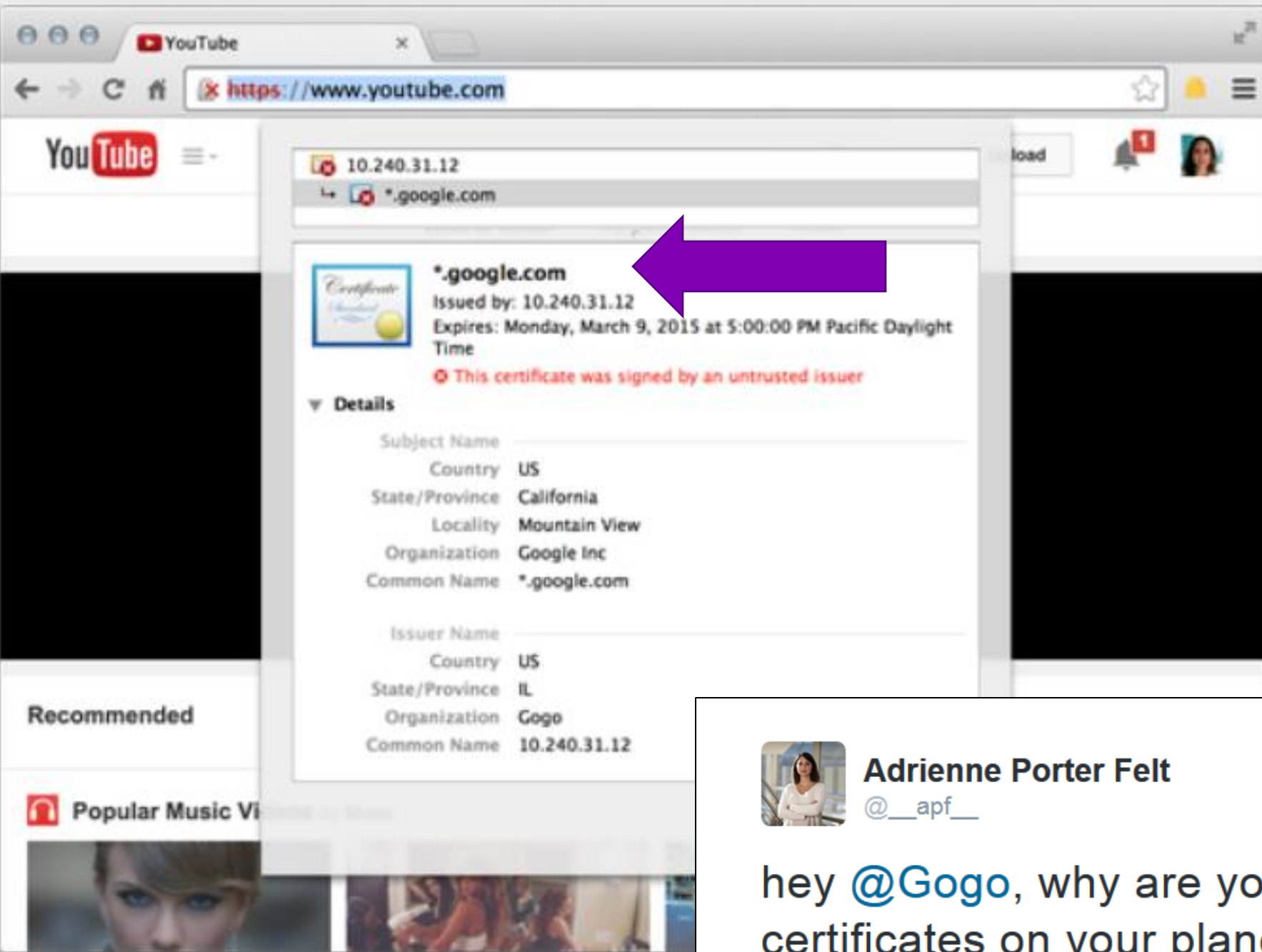


geralt via pixabay

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



Adrienne Porter Felt

@__apf__



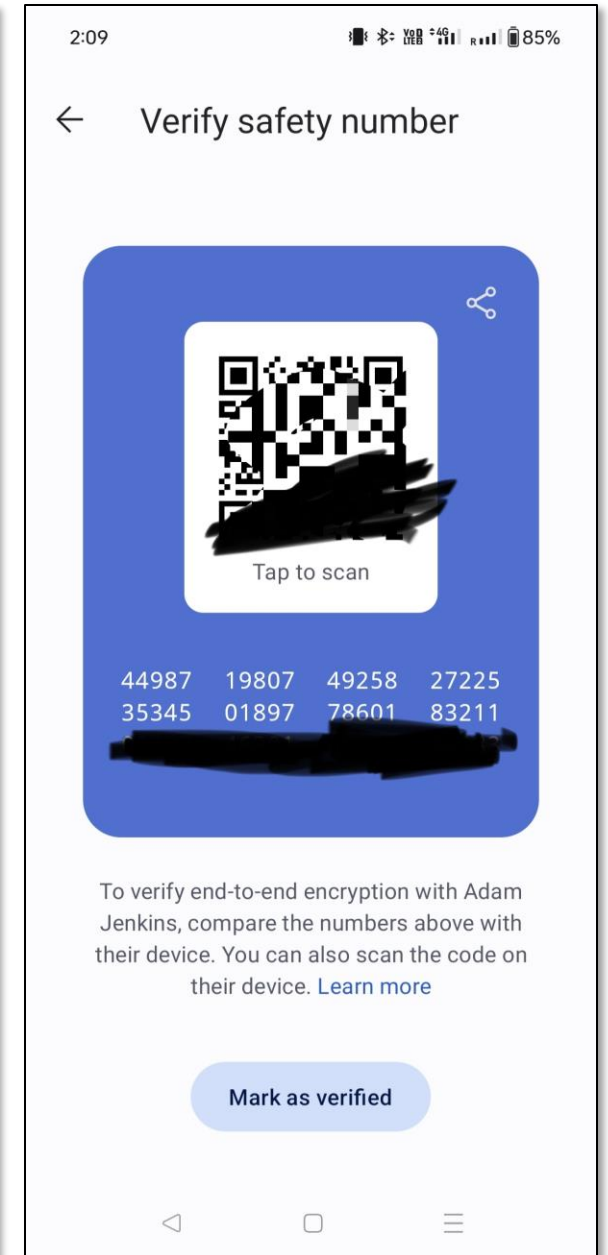
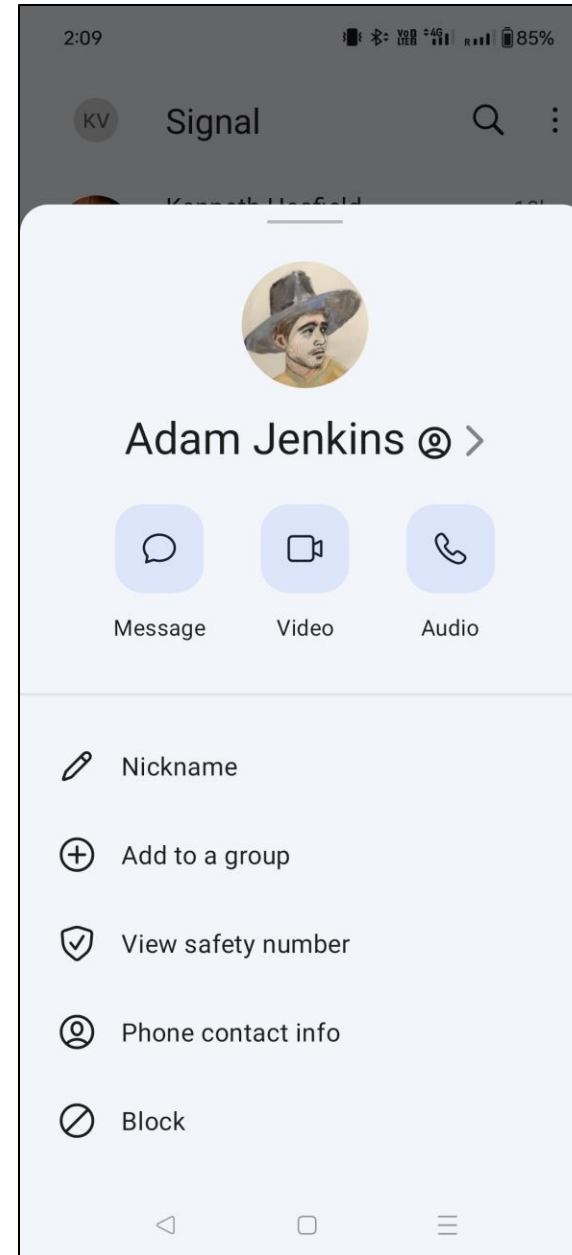
Following

hey @Gogo, why are you issuing *.google.com certificates on your planes?

END-TO-END MESSAGING

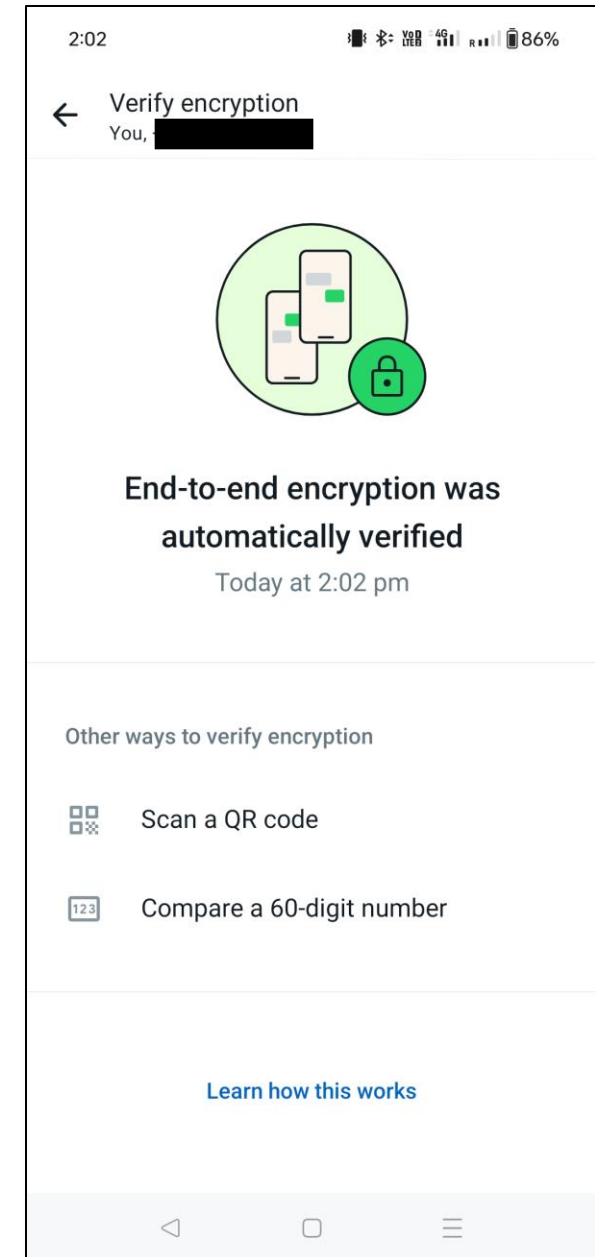
Signal

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



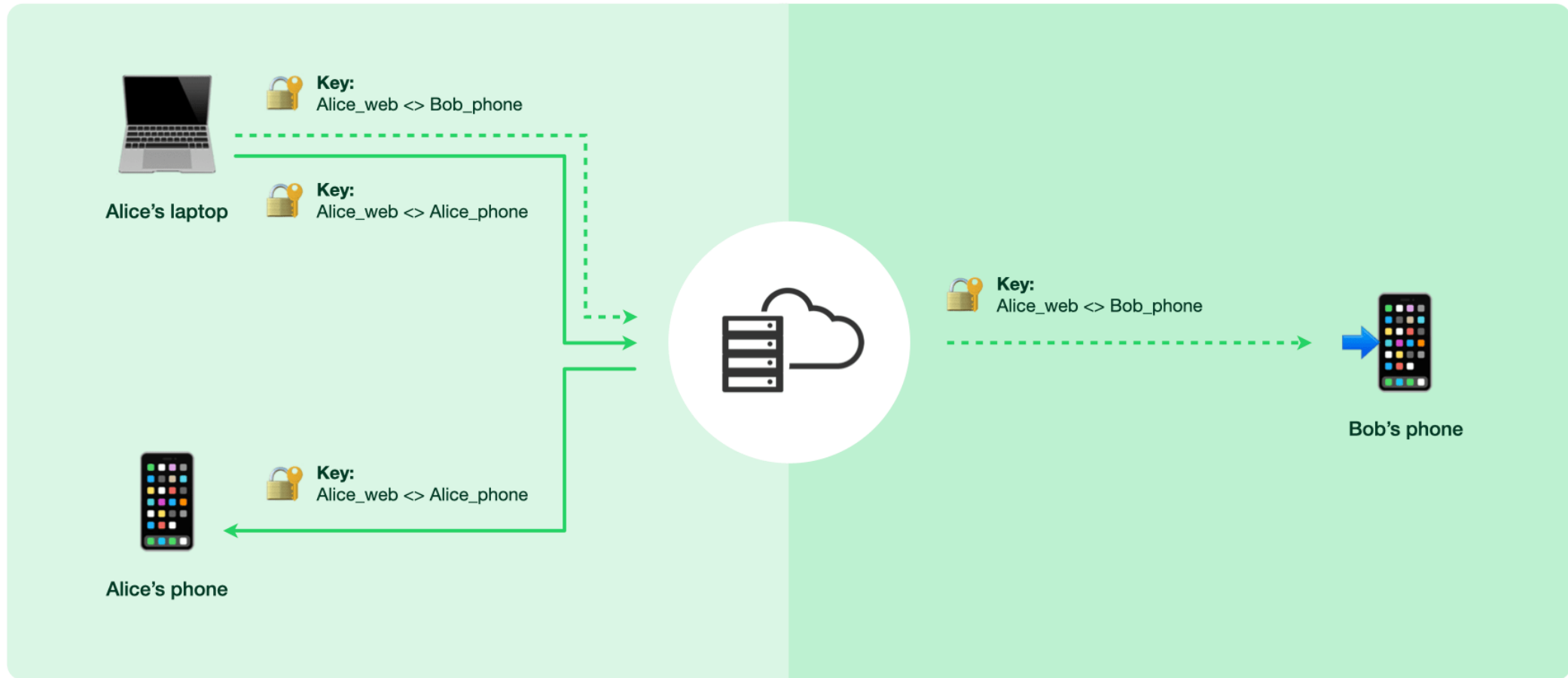
WhatsApp

- 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/>

QUESTIONS