AIN'T NO PARTY LIKE A

CRYPTOPARTY

VISIT HTTPS://GITHUB.COM/YSTVNS/CRYPTOPARTIES TO FOLLOW ALONG!

INTRODUCTION

- It’s easy and realistic to improve your digital security in a meaningful way, even for beginners.
- It’s impossible to achieve perfect security, even for experts.
- By understanding (1) how digital communications technology works and (2) the kinds of risks you’re exposed to, you can make better choices about how to protect yourself and your future clients’ information.
- Format: 25 minute presentation, 35 minutes hands-on training.

UNDERSTANDING RISKS

- State surveillance, police and intelligence agencies, political profiling, censorship, criminal investigation.
- Behavioural tracking, data mining, targeted advertising, social network mapping, sale of personal data to third parties.
- Identity theft, fraud, account hijacking, corporate espionage, tampered digital records, data breach and loss, exposure of privileged information and client confidentiality.
- Extortion, eavesdropping, emotional abuse and harassment.

FOUR “LEVELS” OF RISK TO CONSIDER

- Security of the **network**
- Security of the **message** itself
- Security of your **device** (like a phone or computer)
- Security of the **people** involved
- We’re going to use these four “levels” of risk to provide a framework for today’s workshop.

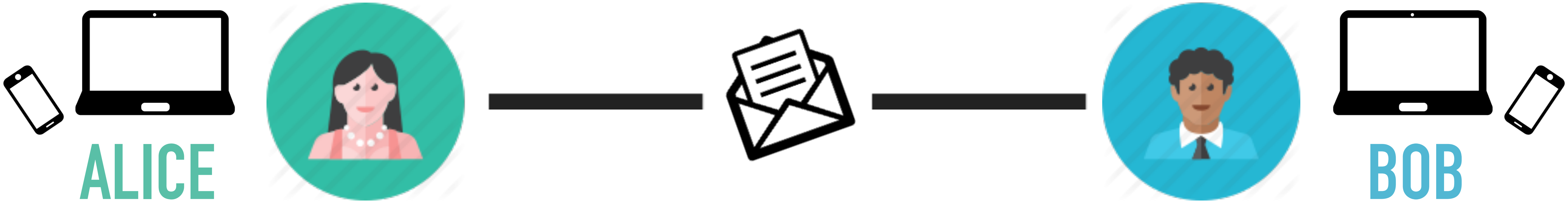
A huge thanks to Lex Gill and …

LET'S DO THIS!

- We'll eventually split up into two groups to learn specific tools.
- Group 1 – more secure browsing:

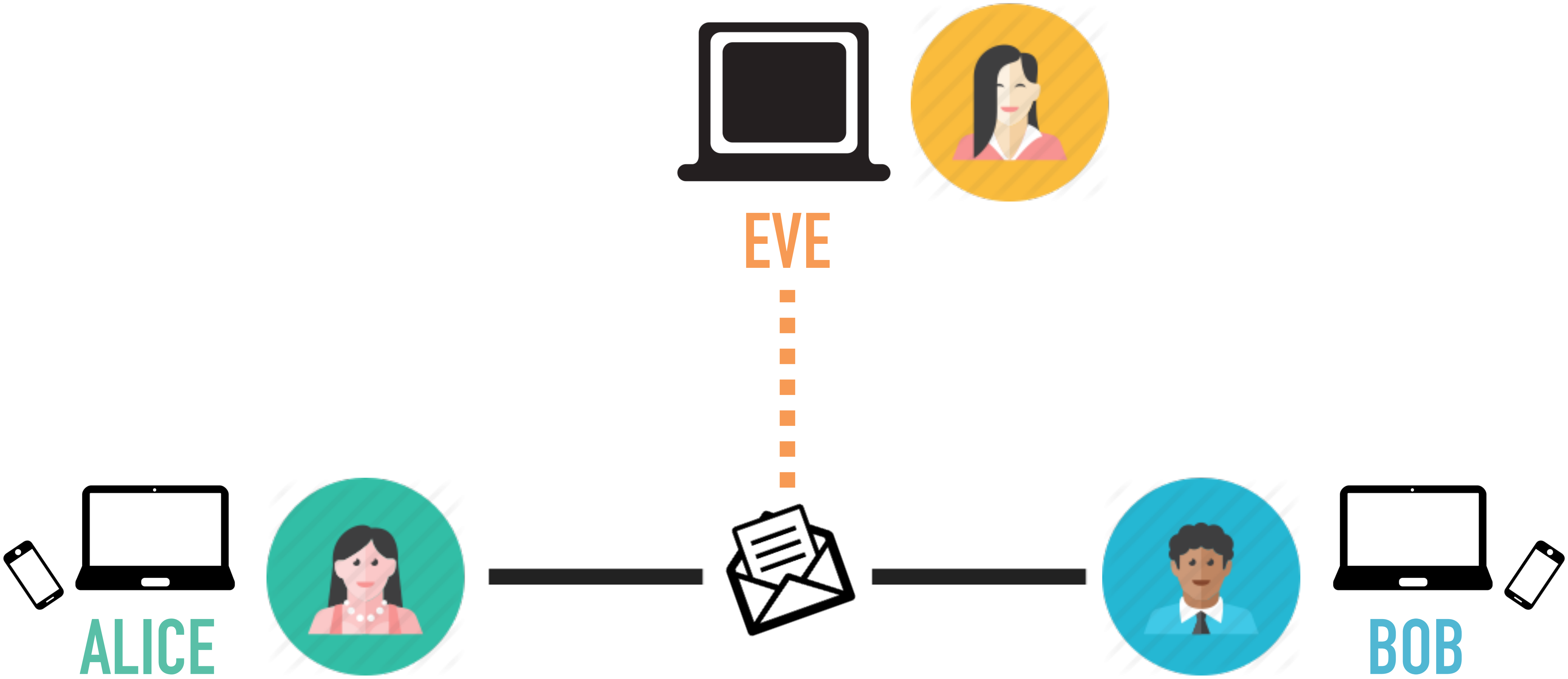
  - download Tor Browser (www.torproject.org)
  - DuckDuckGo (visit duckduckgo.com)
- Group 2 – more private communication:

  - Signal (Encrypted SMS) (download the app on iOS or Android)
  - PGP (Encrypted emails) (PC users instructions here, Mac users here, Linux users here – choose which email you'd like to use for encrypted email and find out its IMAP/POP instructions, and download Thunderbird!)



ALICE

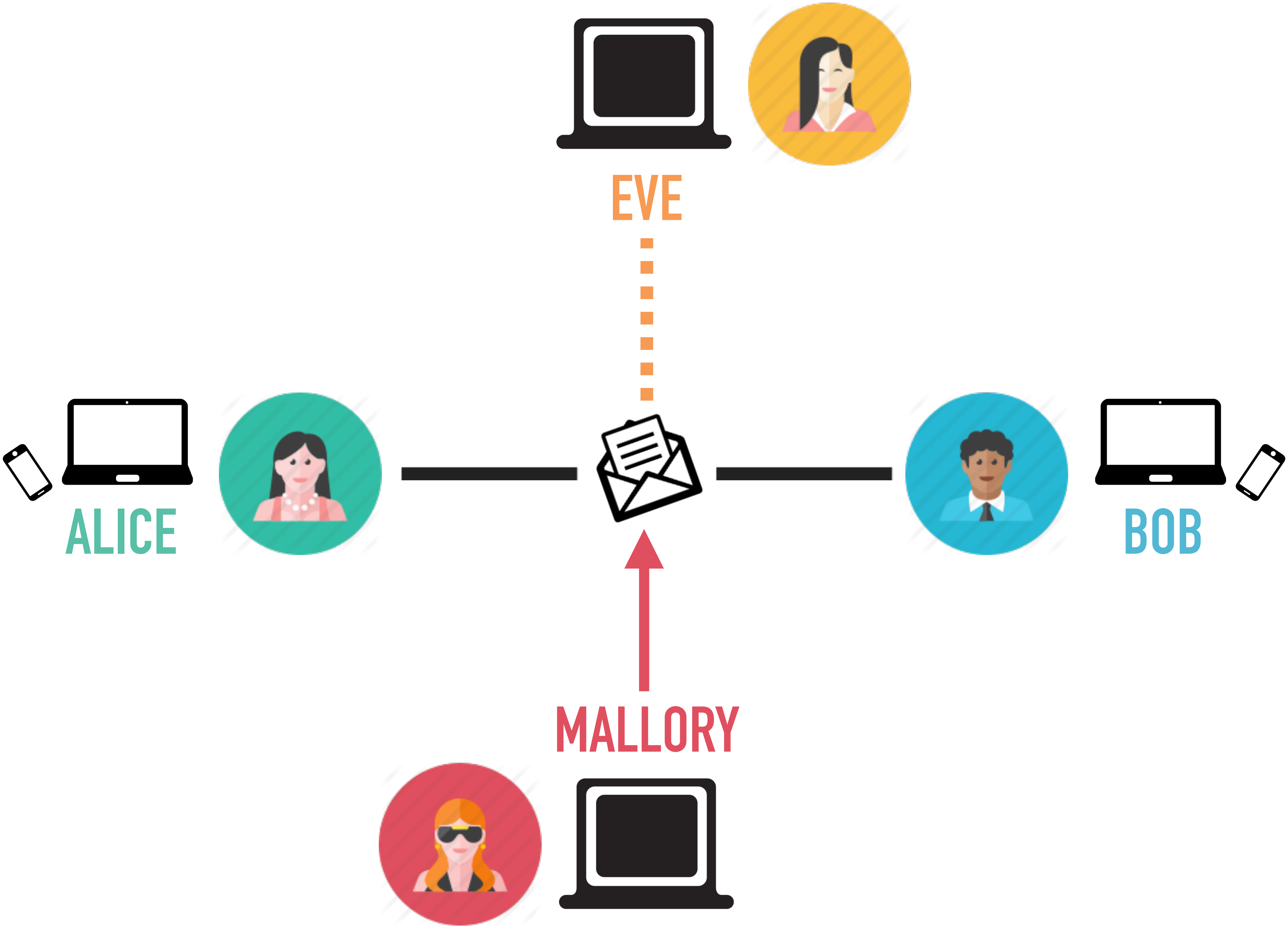
BOB



EVE

ALICE

BOB


EVE
ALICE
BOB
MALLORY

WHAT IS ENCRYPTION?

- Encryption is the process of scrambling data using complex mathematics.
- Encryption makes your data look like random gibberish, which can only be reconstituted if you possess a decryption key. Decrypting without the key is extremely difficult (like, it will take millions of billions of years).
- Encryption is rarely the weakest link. Breaches usually occur because of something else, often human error.

NETWORK SECURITY

- What? Blocking sites that track you and encrypting your internet traffic.

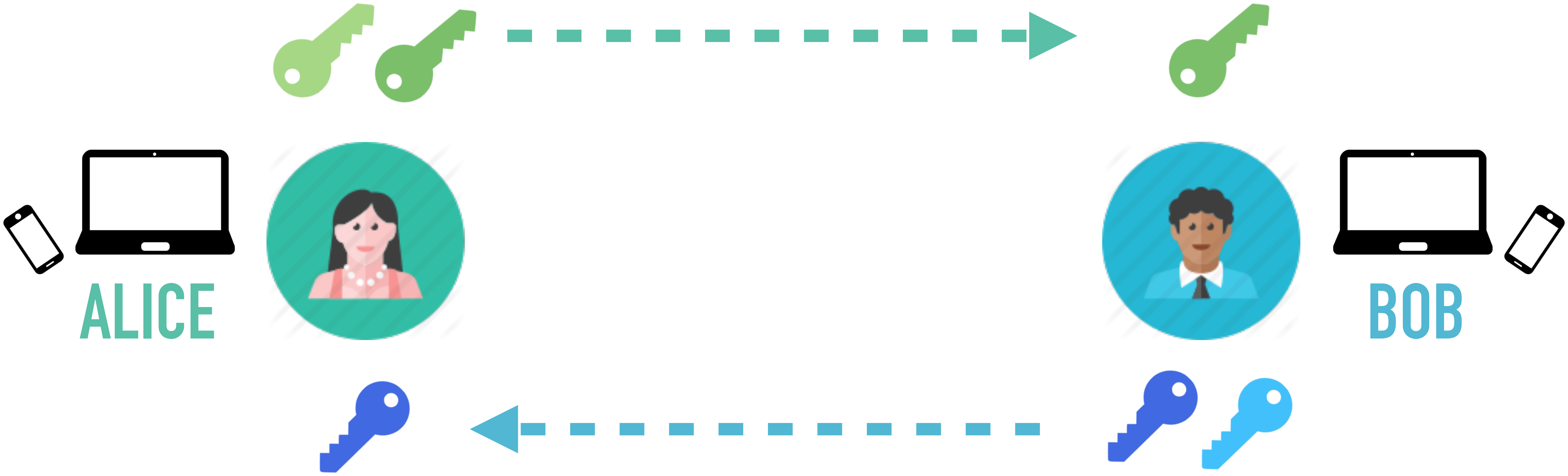
- Why? Helps protect against behavioural tracking, account hijacking, censorship, social network mapping, eavesdropping, and advertising.

- How?
  - Encrypt your connection (HTTPS everywhere, etc.)
  - Block outgoing or incoming connections (ad blockers, Privacy Badger, firewalls, etc.)
  - Tunnel traffic (Virtual Private Networks, Tor, etc.)

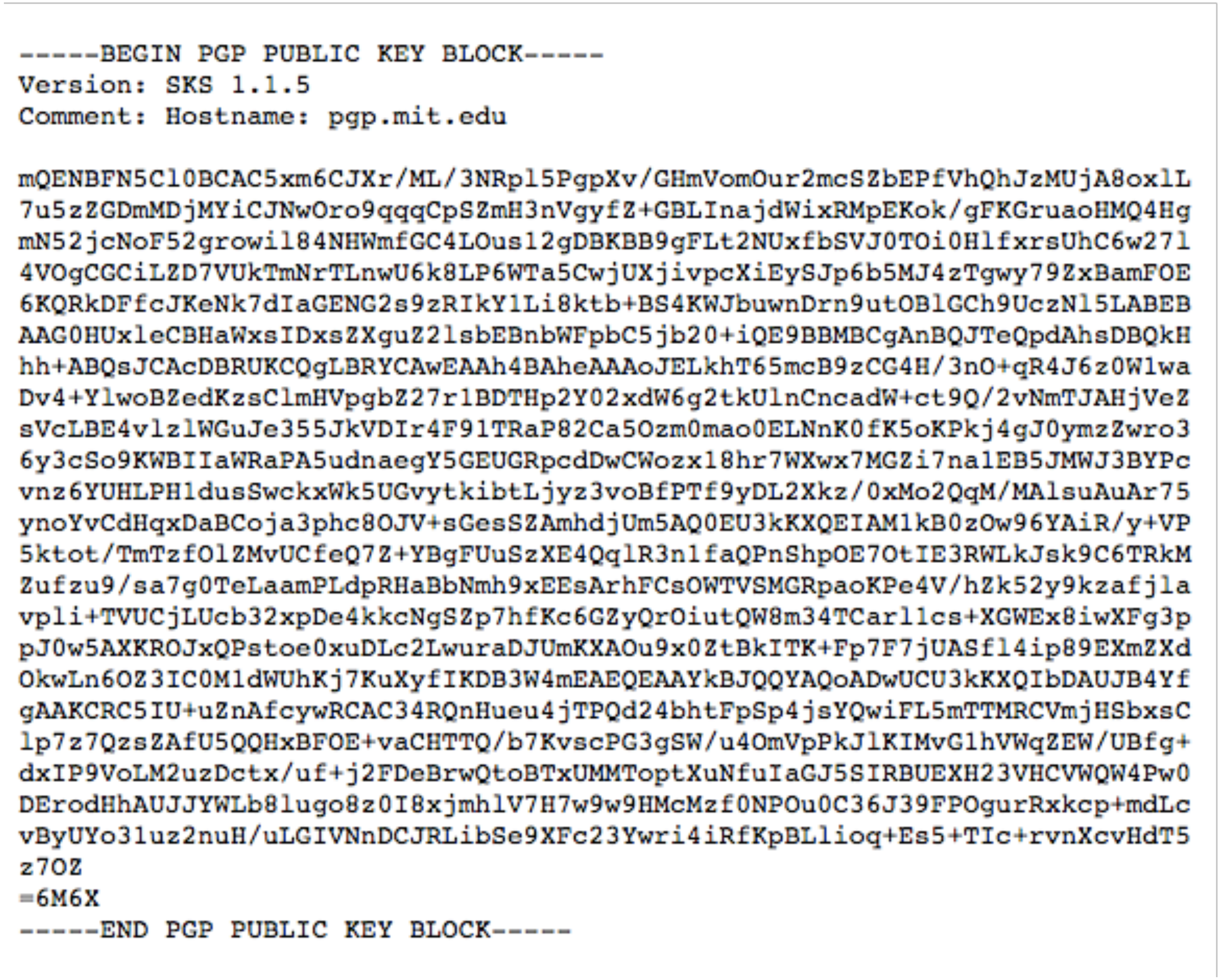
MESSAGE SECURITY

- What? Ways to encrypt individual messages you send and receive.
- Why? Required if you want to ensure the confidentiality of a particular message while stored and transmitted.
- How?
  - Encrypt the message end-to end (PGP for email, Signal for text messaging, OTR for instant messaging)
  - Authenticate the recipient's identity

Alice and Bob each generate a pair of keys.
They each have a **private key** and a **public key**.



Alice sends Bob a copy of her public key.
Bob sends Alice a copy of his public key.
Their **private** keys stay secret.

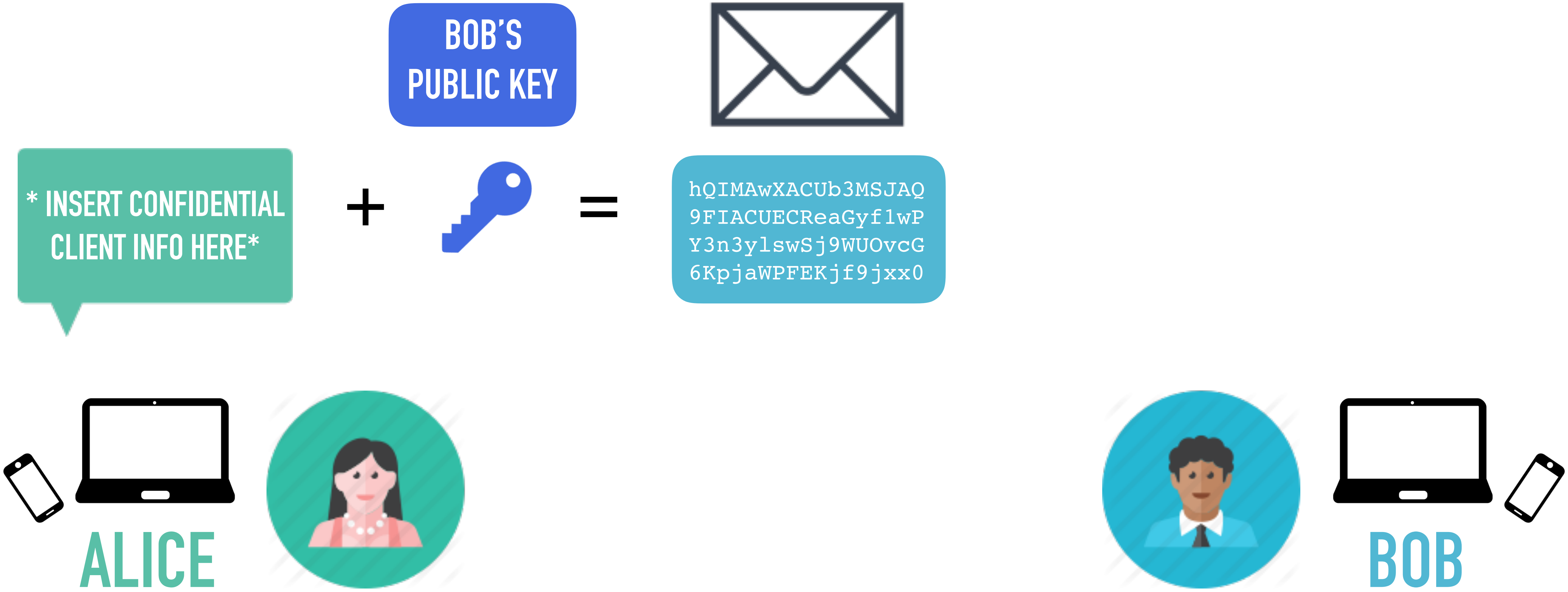


```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: SKS 1.1.5
Comment: Hostname: pgp.mit.edu

mQENBFN5Cl0BCAC5xm6CJXr/ML/3NRpl5PgpXv/GHmVomOur2mcSZbEPfVhQhJzMUjA8oxlL
7u5zZGDmMDjMYiCJNwOro9qqqCpSZmH3nVgyfZ+GBLInajdWixRMpEKok/gFKGruaoHMQ4Hg
mN52jcNoF52growil84NHWmfGC4LOus12gDBKBB9gFLt2NUxfbSVJ0TOi0HlfxrsUhC6w27l
4VOgCGCiLZD7VUkTmNrTLnwU6k8LP6WTa5CwjUXjivpcXiEySJp6b5MJ4zTgwy79ZxBamFOE
6KQRkDFfcJKeNk7dIaGENG2s9zRIkY1Li8ktb+BS4KWJbuwnDrn9utOBlGCh9UczNl5LABEB
AAG0HUxleCBHaWxsIDxsZXguZ2lsbEBnbWFpbC5jb20+iQE9BBMBCgAnBQJTeQpdAhsDBQkH
hh+ABQsJCAcDBRUKCQgLBRYCAwEAAh4BAheAAAoJELkhT65mcB9zCG4H/3nO+qR4J6z0W1wa
Dv4+YlwoBZedKzsClmHVpgbZ27r1BDTHp2Y02xdW6g2tkUlnCncadW+ct9Q/2vNmTJAHjVeZ
sVcLBE4vlzlWGuJe355JkVDIr4F91TRaP82Ca5Ozm0mao0ELNnK0fK5oKPkj4gJ0ymzZwro3
6y3cSo9KWBIIaWRaPA5udnaegY5GEUGRpcdDwCWozx18hr7WXwx7MGZi7na1EB5JMWJ3BYPc
vnz6YUHLPH1dusSwckxWk5UGvytkibtLjyz3voBfPTf9yDL2Xkz/0xMo2QqM/MAlsuAuAr75
ynoYvCdHqxDaBCoja3phc8OJV+sGesSZAmhdjUm5AQ0EU3kKXQEIAM1kB0zOw96YAiR/y+VP
5ktot/TmTzfOlZMvUCfeQ7Z+YBgFUuSzXE4QqlR3n1faQPnShpOE7OtIE3RWLkJsk9C6TRkM
Zufzu9/sa7g0TeLaamPLdpRHaBbNmh9xEEsArhFCsOWTVSMGRpaoKPe4V/hZk52y9kzafjla
vpli+TVUCjLUcb32xpDe4kkcNgSZp7hfKc6GZyQrOiutQW8m34TCarllcs+XGWEx8iwXFg3p
pJ0w5AXKROJxQPstoe0xuDLc2LwuraDJUmKXAOu9x0ZtBkITK+Fp7F7jUASfl4ip89EXmZXd
OkwLn6OZ3IC0M1dWUhKj7KuXyfIKDB3W4mEAEQEAAYkBJQQYAQoADwUCU3kKXQIbDAUJB4Yf
gAAKCRC5IU+uZnAfcywRCAC34RQnHueu4jTPQd24bhtFpSp4jsYQwiFL5mTTMRCVmjHSbxsC
lp7z7QzsZAfU5QQHxBFOE+vaCHTTQ/b7KvscPG3gSW/u4OmVpPkJlKIMvG1hVWqZEW/UBfg+
dxIP9VoLM2uzDctx/uf+j2FDeBrwQtoBTxUMMToptXuNfuIaGJ5SIRBUEXH23VHCVWQW4Pw0
DErodHhAUJJYWLb8lugo8z0I8xjmhlV7H7w9w9HMcMzf0NPOu0C36J39FPOgurRxkcp+mdLc
vByUYo3luz2nuH/uLGIVNnDCJRLibSe9XFc23Ywri4iRfKpBLlioq+Es5+TIc+rvnXcvHdT5
z7OZ
=6M6X
-----END PGP PUBLIC KEY BLOCK-----
```

This is what a **public key** looks like.

Alice wants to send a message over the Internet to Bob.



BOB'S PUBLIC KEY

* INSERT CONFIDENTIAL CLIENT INFO HERE*

+

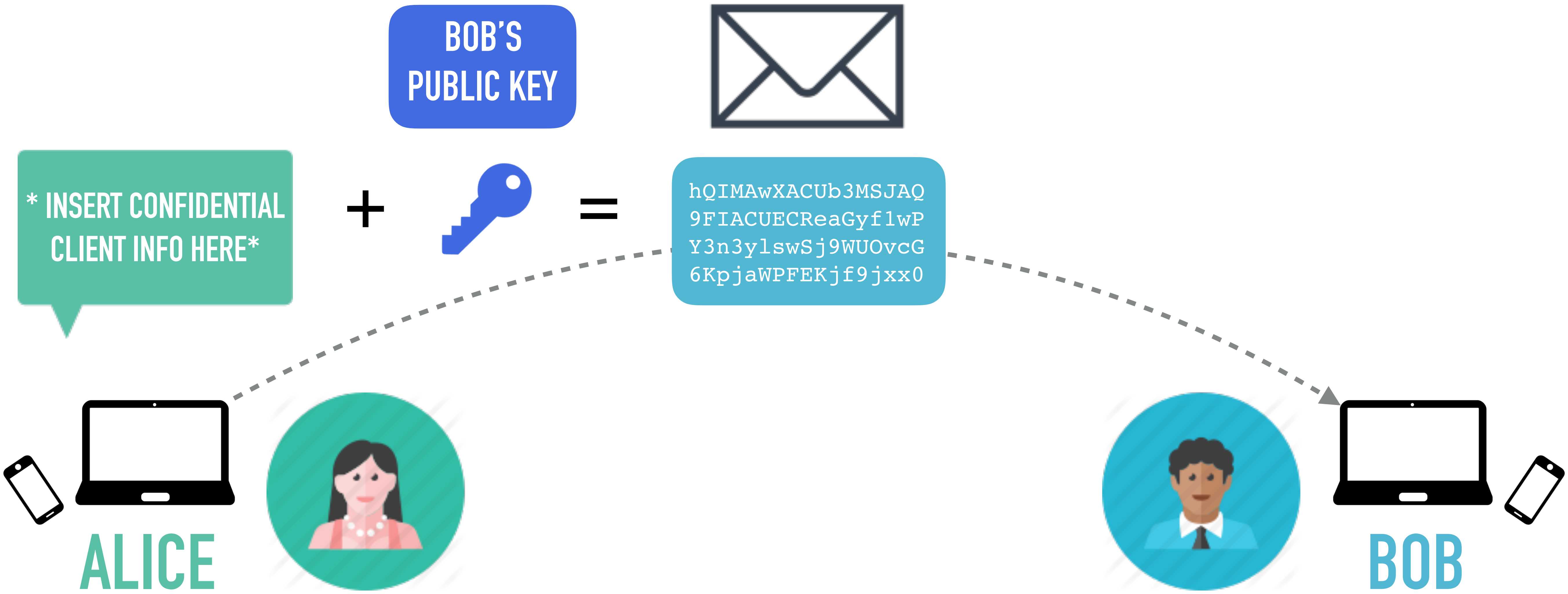
=

```
hQIMAwXACUb3MSJAQ
9FIACUECReaGyf1wP
Y3n3ylswSj9WUOvcG
6KpjaWPFEKjf9jxx0
```

ALICE

BOB

Alice wants to send a message
over the Internet to Bob.



BOB’S
PUBLIC KEY

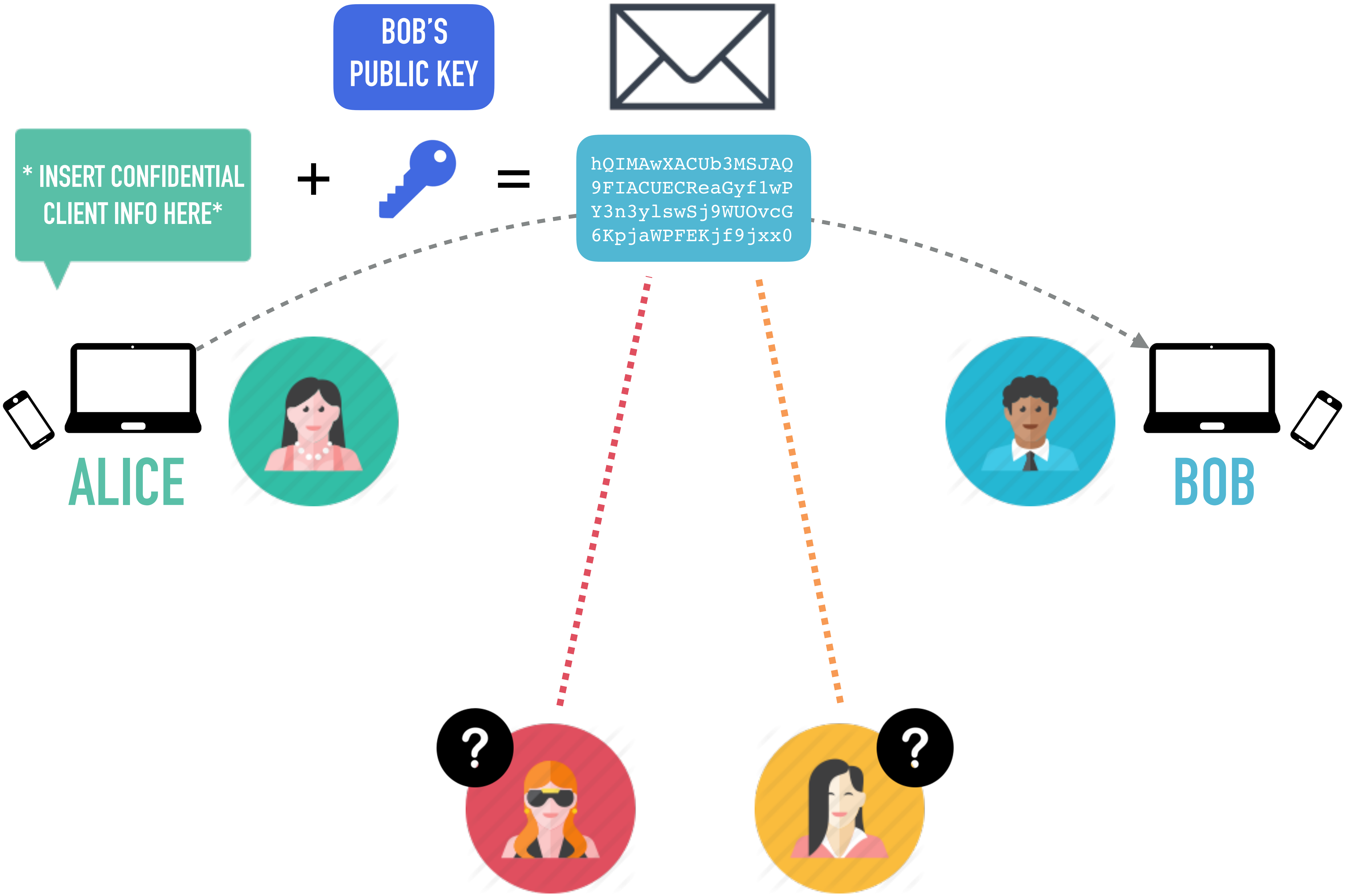
* INSERT CONFIDENTIAL
CLIENT INFO HERE*

+ =

```
hQIMAwXACUb3MSJAQ
9FIACUECReaGyf1wP
Y3n3ylswSj9WUOvcG
6KpjaWPFEKjf9jxx0
```

ALICE

BOB



BOB'S PUBLIC KEY

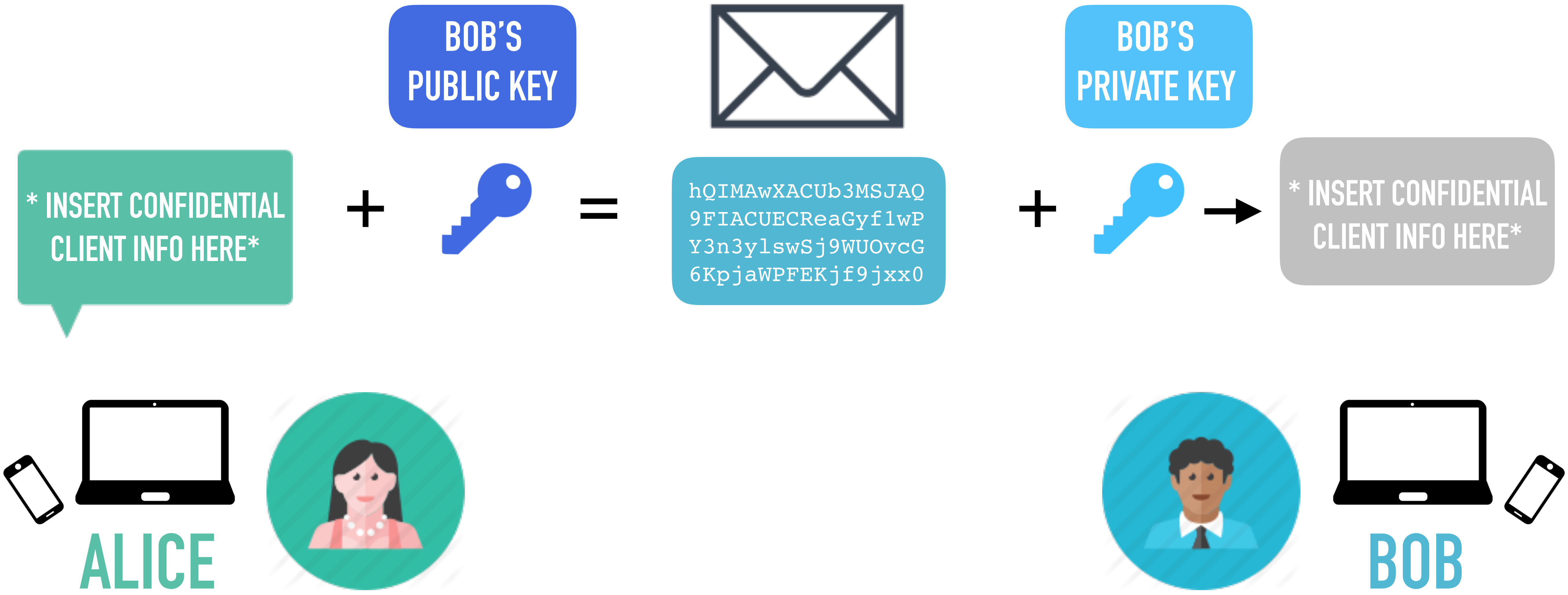
* INSERT CONFIDENTIAL CLIENT INFO HERE*

+ =

hQIMAwXACUb3MSJAQ
9FIACUECReaGyf1wP
Y3n3ylswSj9WUOvcG
6KpjaWPFEKjf9jxx0

ALICE

BOB



BOB'S PUBLIC KEY

BOB'S PRIVATE KEY

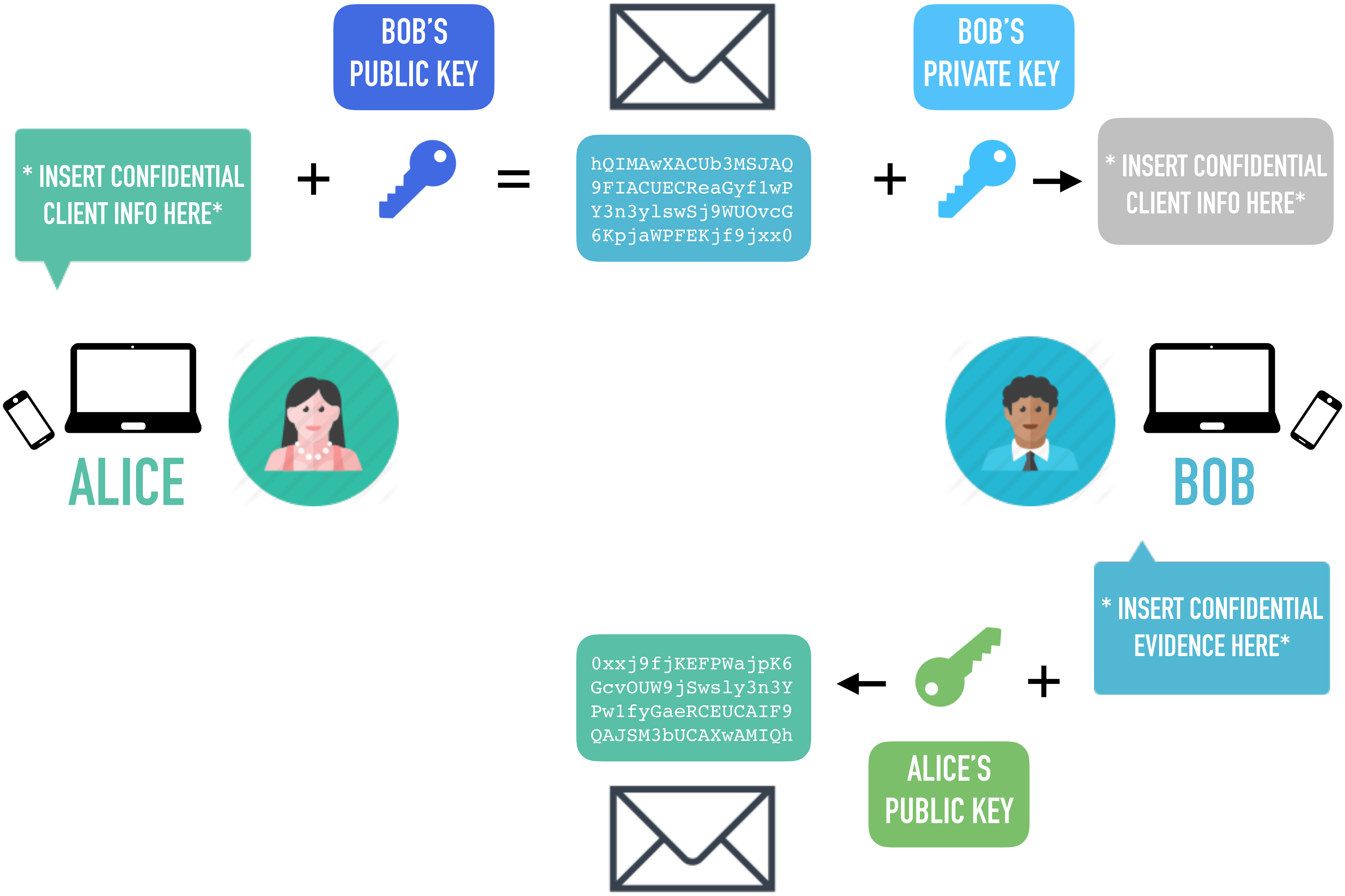
* INSERT CONFIDENTIAL CLIENT INFO HERE* + =

hQIMAwXACUb3MSJAQ
9FIACUECReaGyf1wP
Y3n3ylswSj9WUOvcG
6KpjaWPFEKjf9jxx0

+ → * INSERT CONFIDENTIAL CLIENT INFO HERE*

ALICE

BOB



BOB'S PUBLIC KEY

BOB'S PRIVATE KEY

* INSERT CONFIDENTIAL CLIENT INFO HERE*

+

=

```
hQIMAwXACUb3MSJAQ
9FIACUECReaGyf1wP
Y3n3ylswSj9WUOvcG
6KpjaWPFEKjf9jxx0
```

+ →

* INSERT CONFIDENTIAL CLIENT INFO HERE*

ALICE

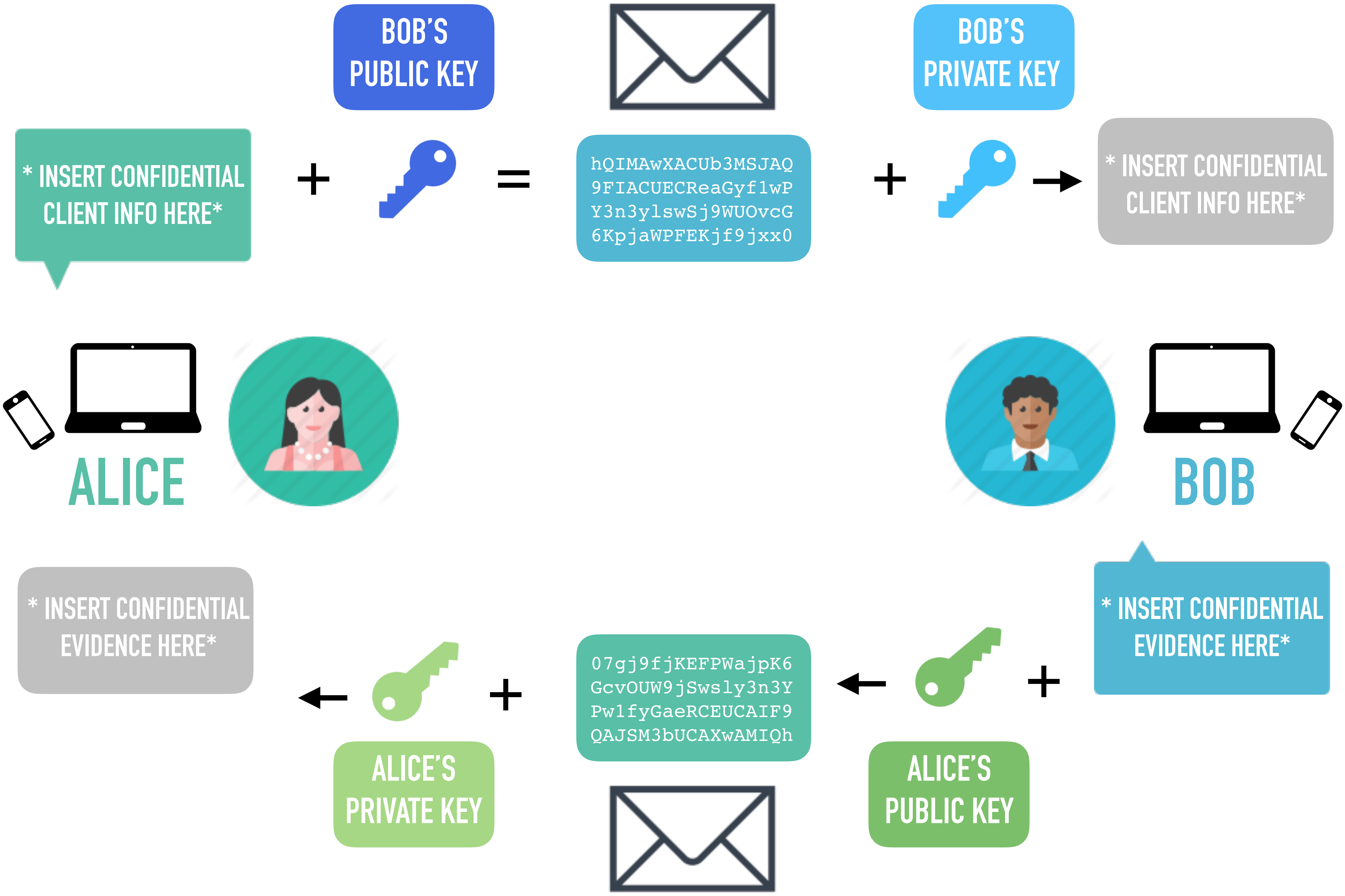
BOB

* INSERT CONFIDENTIAL EVIDENCE HERE*

+ ←

```
0xxj9fjKEFPWajpK6
GcvOUW9jSwsly3n3Y
Pw1fyGaeRCEUCAIF9
QAJSM3bUCAXwAMIQh
```

ALICE'S PUBLIC KEY



* INSERT CONFIDENTIAL CLIENT INFO HERE* + BOB'S PUBLIC KEY =

```
hQIMAwXACUb3MSJAQ
9FIACUECReaGyf1wP
Y3n3ylswSj9WUOvcG
6KpjaWPFEKjf9jxx0
```

+ BOB'S PRIVATE KEY → * INSERT CONFIDENTIAL CLIENT INFO HERE*

ALICE

BOB

* INSERT CONFIDENTIAL EVIDENCE HERE* + ALICE'S PUBLIC KEY →

```
07gj9fjKEFPWajpK6
GcvOUW9jSwsly3n3Y
Pw1fyGaeRCEUCAIF9
QAJSM3bUCAXwAMIQh
```

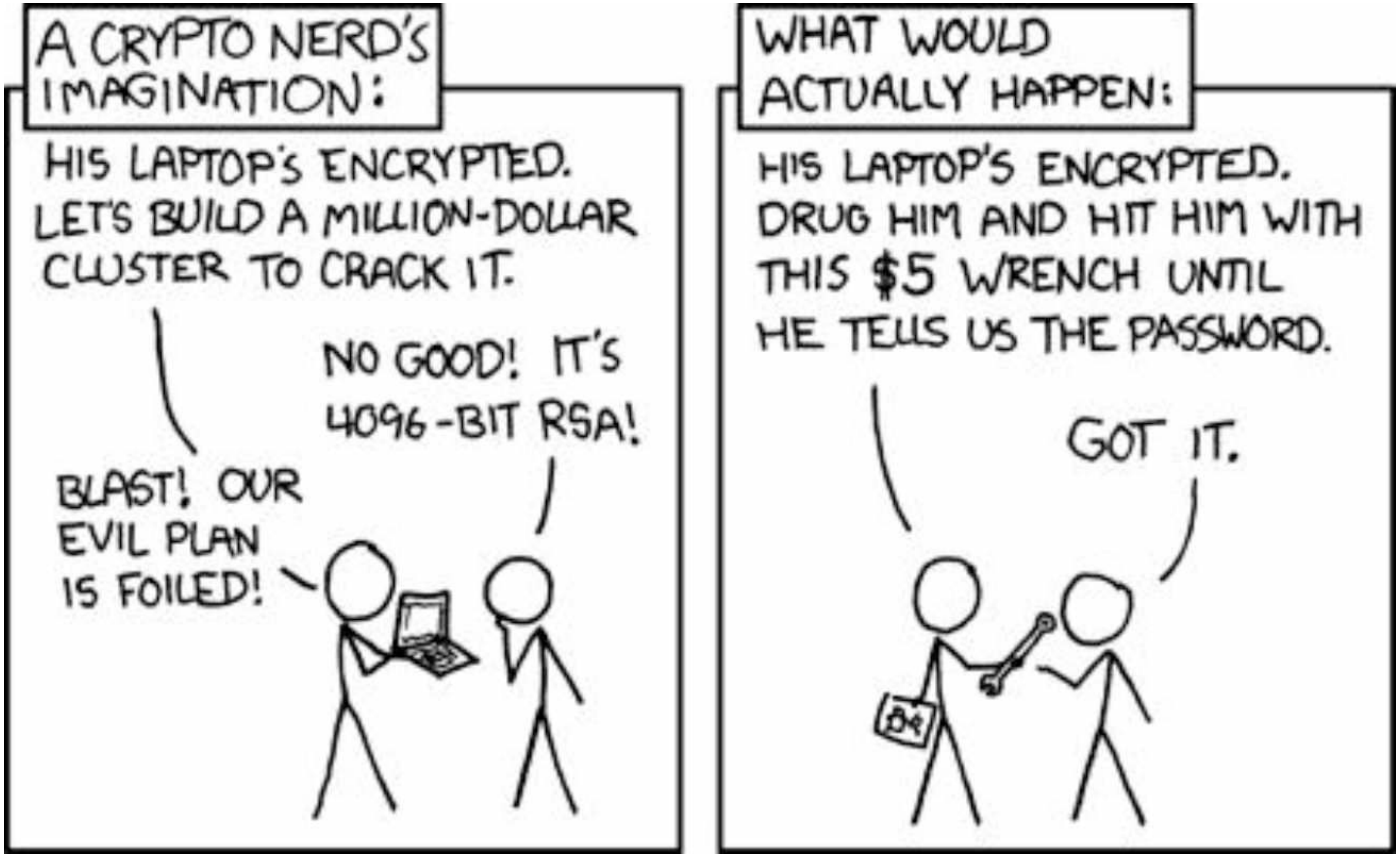
+ ALICE'S PRIVATE KEY → * INSERT CONFIDENTIAL EVIDENCE HERE*

SOME RECOMMENDATIONS FOR ENCRYPTED MESSAGING

- Keep your private key safe and confidential. Use a strong passphrase for your key.
- Remember that encrypting your emails:
  does not hide your identity
  does not hide the subject line
  may and probably will attract additional attention
- If your device or that of the recipient is compromised, your conversation is also likely compromised.

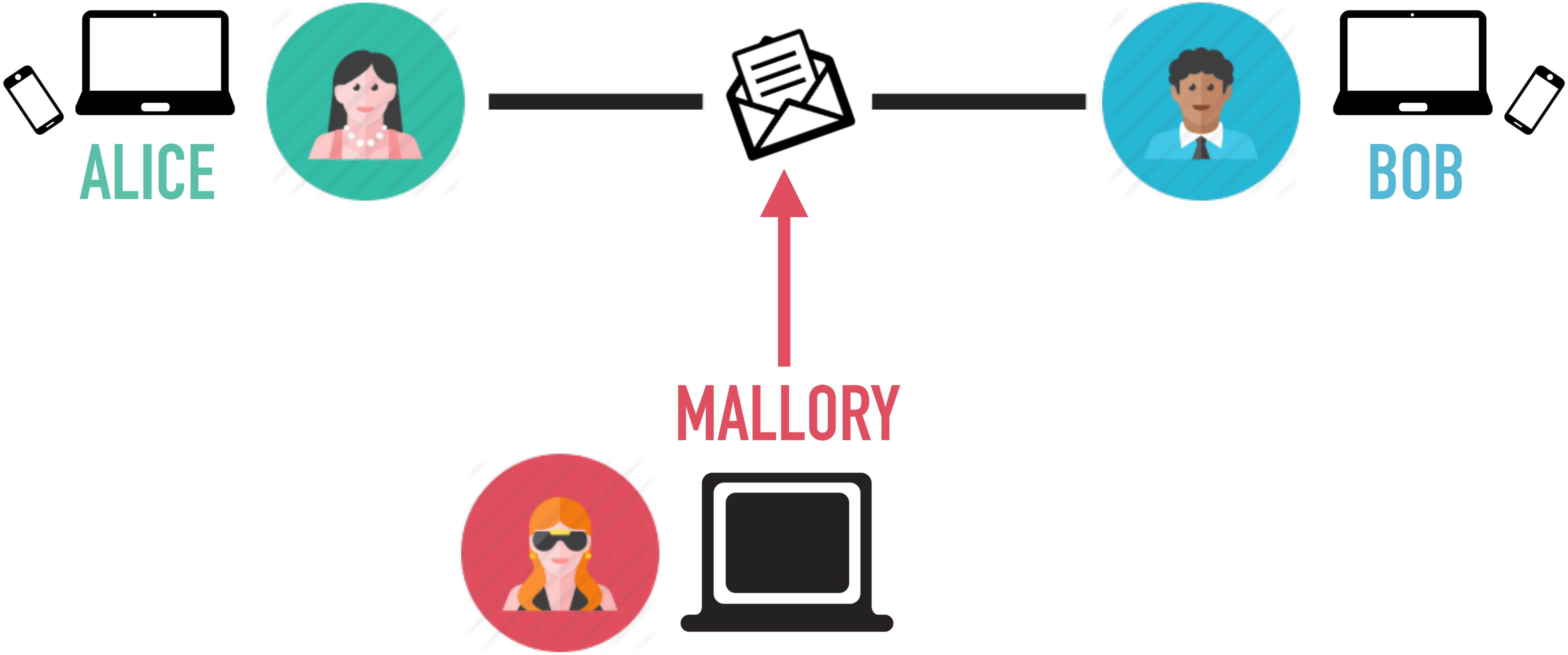
> ENCRYPTION WORKS. PROPERLY IMPLEMENTED STRONG CRYPTO SYSTEMS ARE ONE OF THE FEW THINGS THAT YOU CAN RELY ON. UNFORTUNATELY, ENDPOINT SECURITY IS SO TERRIFICALLY WEAK THAT NSA CAN FREQUENTLY FIND WAYS AROUND IT.

Edward Snowden

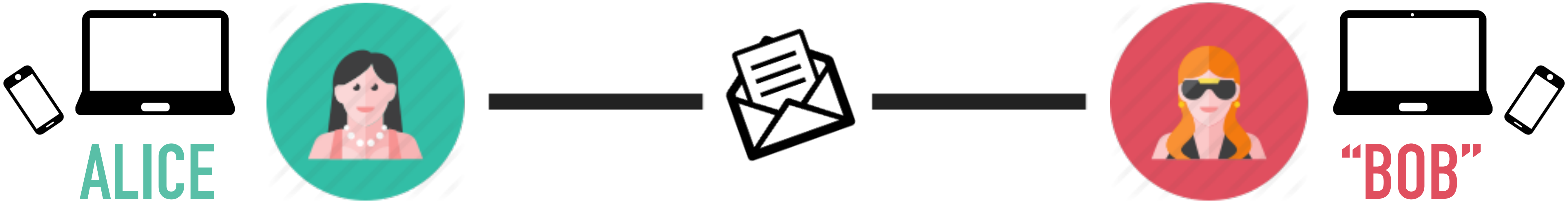

A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Using encryption won't mean perfect security, but it can give you a running start. It forces would-be eavesdroppers and adversaries to do more complex, targeted, and invasive work if they want your data. Or to hit you with a wrench.

Let’s talk about authentication.



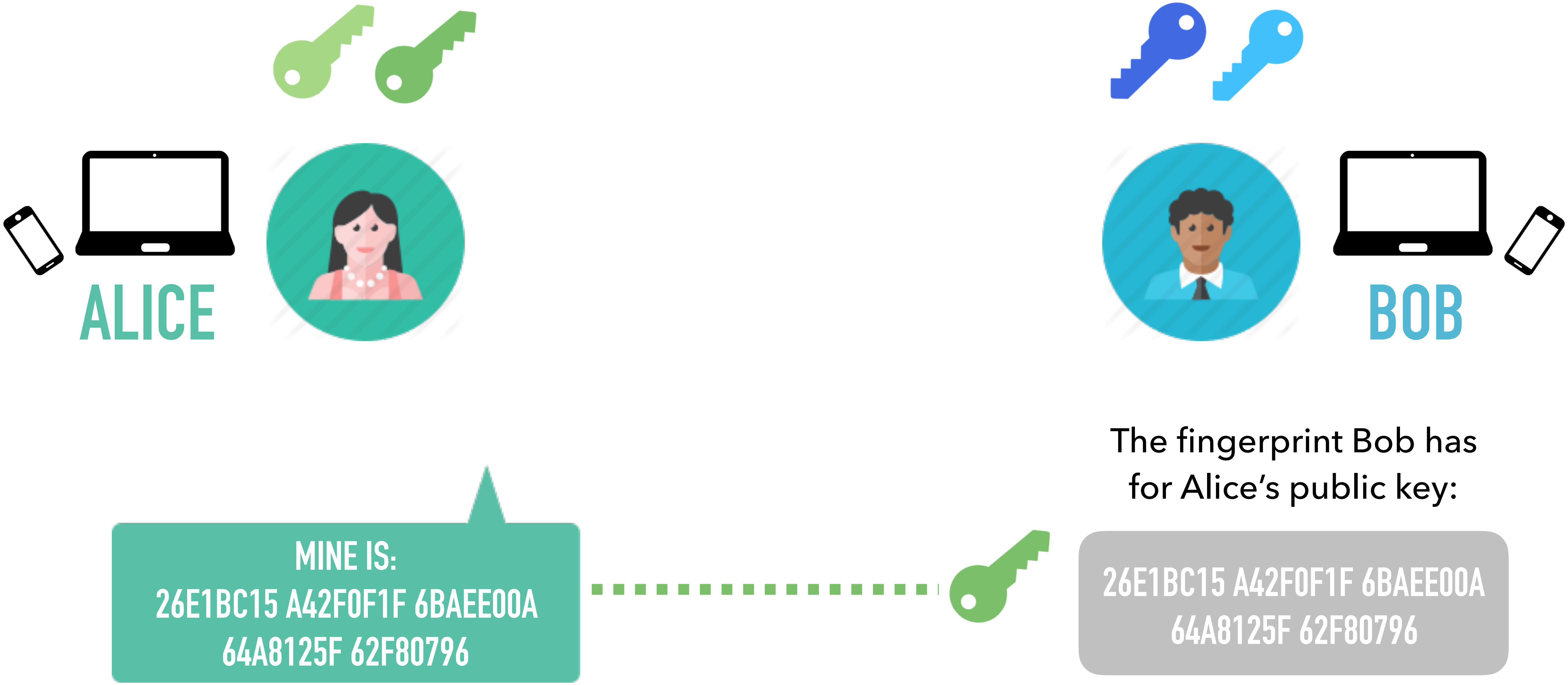
Authentication is about making sure the person you're talking to is actually who they say they are.



An identity using a secure messaging system is usually a public key, often abbreviated as a **fingerprint**.

MINE IS:
26E1BC15 A42F0F1F 6BAEE00A
64A8125F 62F80796

Do they match?

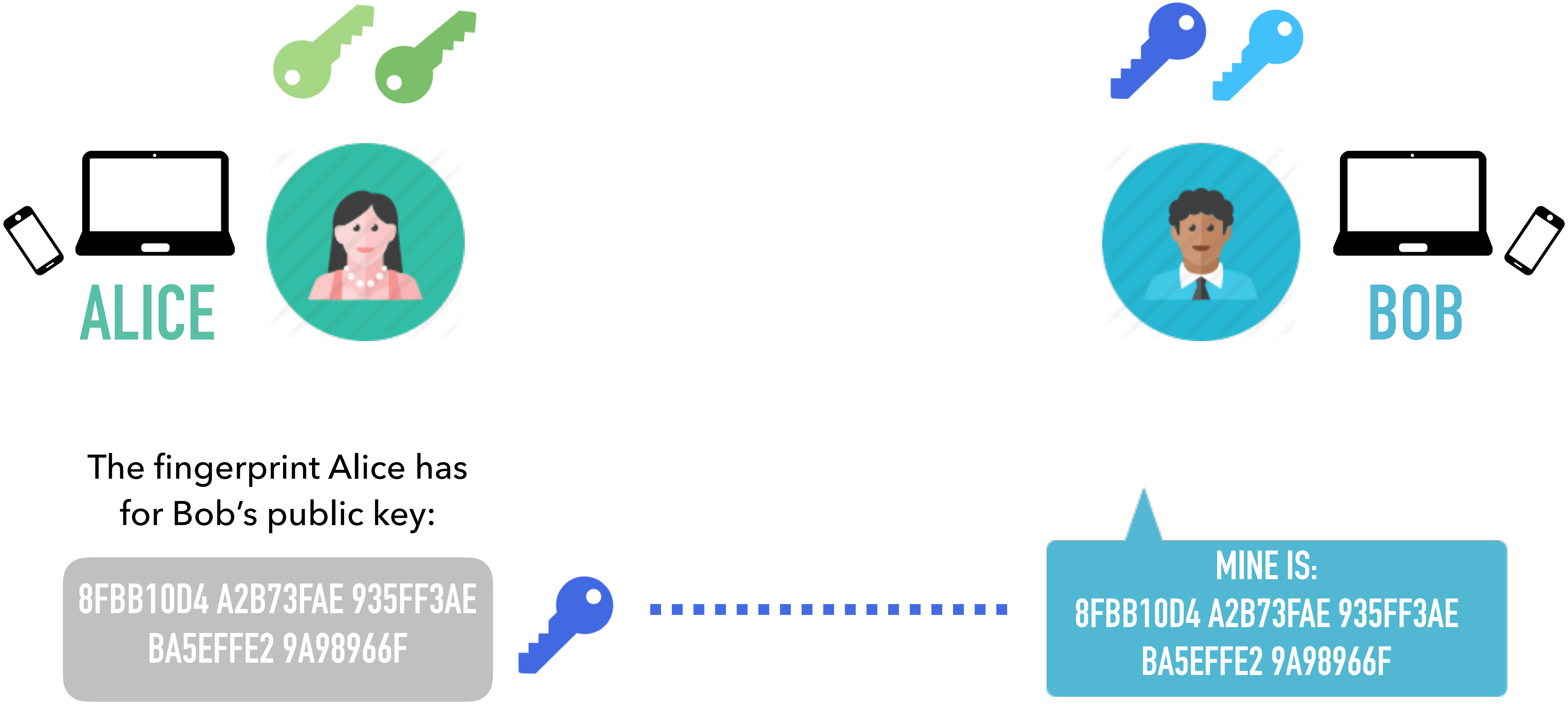


MINE IS:
26E1BC15 A42F0F1F 6BAEE00A
64A8125F 62F80796

The fingerprint Bob has
for Alice’s public key:

26E1BC15 A42F0F1F 6BAEE00A
64A8125F 62F80796

You need to make sure the person you want to talk to has the correct (expected) public key.



ALICE

BOB

The fingerprint Alice has for Bob's public key:

8FBB10D4 A2B73FAE 935FF3AE BA5EFFE2 9A98966F

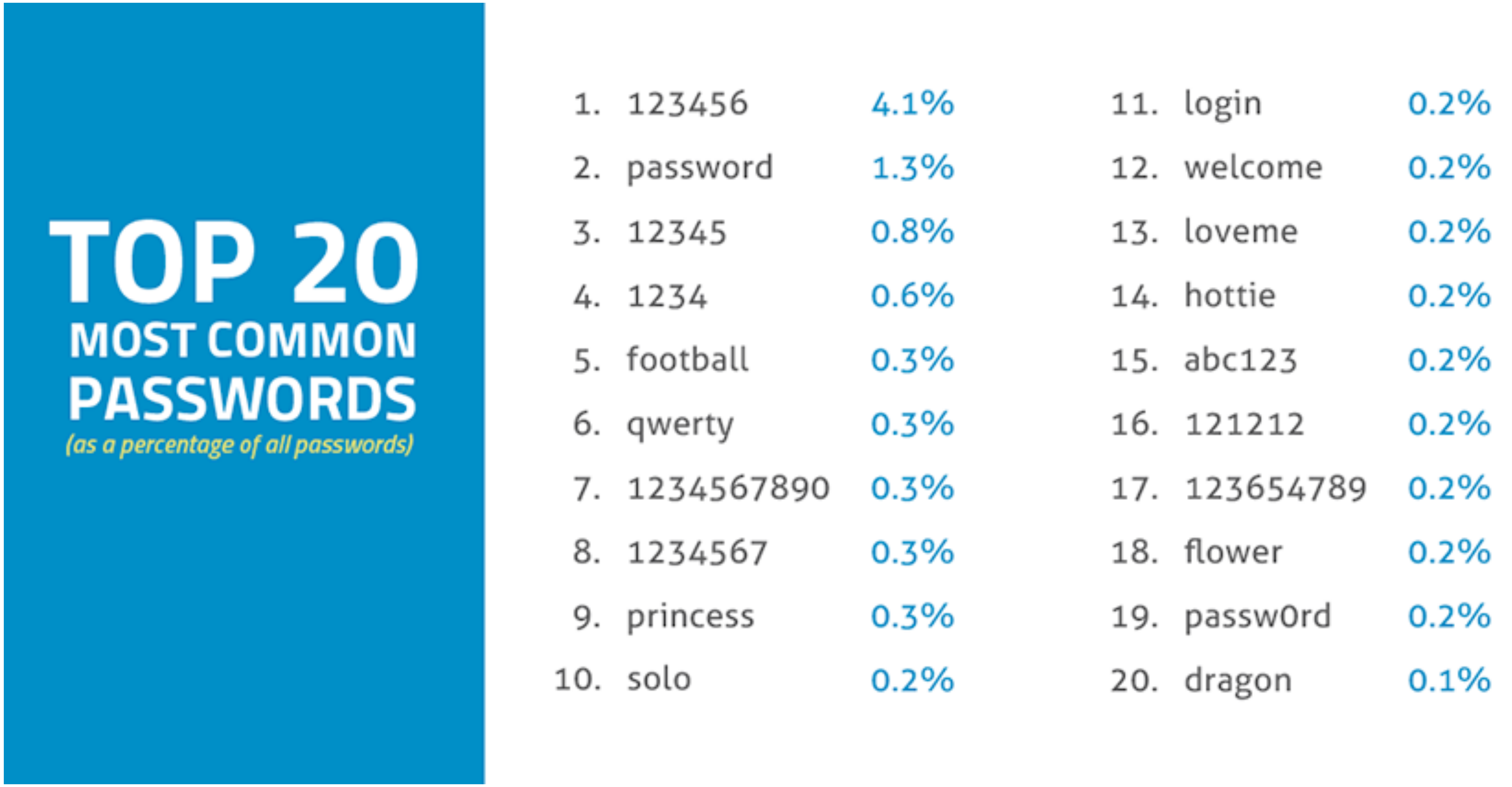
MINE IS: 8FBB10D4 A2B73FAE 935FF3AE BA5EFFE2 9A98966F

DEVICE SECURITY

- What? Steps to make your computer or phone less vulnerable to attack.
- Why? Useful whenever your device might physically fall into the hands of an attacker.
- How?
  - Full disk encryption (for your phone and computer)
  - Secure deletion
  - Regular software updates
  - Firewall, minimum applications installed
  - Use non-persistent OS (e.g.: Tails)
  - Strong password(s)

HUMAN SECURITY

- What? Simple changes you can make to your behaviour.
- Why? Helps prevent human error from being the weak link in any security system.
- How?
  - Stronger passwords and password management
  - Two-factor authentication (for Gmail and other services)
  - Caution about what you share (and who you share with)
  - Strategic choices about where and how you access the Internet (e.g., avoiding shared computers, public/free wifi)
  - Be mindful of phishing and scams (you did not win a million dollars)



TOP 20 MOST COMMON PASSWORDS

(as a percentage of all passwords)

1.	123456	4.1%	11.	login	0.2%
2.	password	1.3%	12.	welcome	0.2%
3.	12345	0.8%	13.	loveme	0.2%
4.	1234	0.6%	14.	hottie	0.2%
5.	football	0.3%	15.	abc123	0.2%
6.	qwerty	0.3%	16.	121212	0.2%
7.	1234567890	0.3%	17.	123654789	0.2%
8.	1234567	0.3%	18.	flower	0.2%
9.	princess	0.3%	19.	passw0rd	0.2%
10.	solo	0.2%	20.	dragon	0.1%

2015, source.

CHOOSING AN AWESOME PASSWORD

- **Unique:** don’t use the same password for everything.
- **Long:** the more numbers, letters & characters the better.
- **Hard to guess:** avoid picking dictionary words.
- **Frequently changed:** every few months, or as soon as you believe it might have been compromised.
- **Confidential:** don’t share your password with anyone.
- **Managed:** seems daunting? Use a password manager.

MORE RESOURCES

- RiseUp.Net, Communications Security https://help.riseup.net/en/security
- EFF, Surveillance Self Defense https://ssd.eff.org/
- Equalit.ie, Digital Security Lessons https://learn.equalit.ie/wiki/Online_Learning
- Tactical Tech, Security in a Box https://securityinabox.org/en
- Freedom of the Press Foundation, Encryption Works https://github.com/freedomofpress/encryption-works/blob/master/encryption_works.md
- Tactical Tech, Gender and Security https://gendersec.tacticaltech.org/wiki/index.php/Main_Page

LET'S DO THIS!

- Let's split up into two groups to learn specific tools.
- Group 1 – more secure browsing:

  - download Tor Browser (www.torproject.org)
  - DuckDuckGo (visit duckduckgo.com)
- Group 2 – more private communication:

  - Signal (Encrypted SMS) (download the app on iOS or Android)
  - PGP (Encrypted emails) (PC users instructions here, Mac users here, Linux users here – choose which email you'd like to use for encrypted email and find out its IMAP/POP instructions!)

THANK YOU!

Visit https://github.com/ystvns/cryptoparties to find this presentation online.

Feel free to follow me on twitter – @yystvns :)