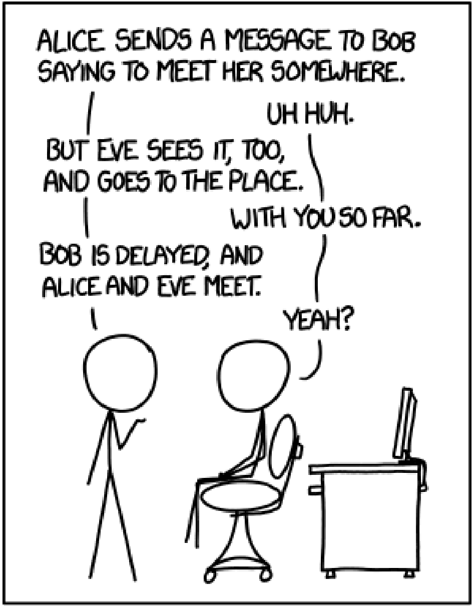
Crypto Tales from the Trenches

Julia Angwin, Jack Gillum, Laura Poitras

(also Nadia Heninger)

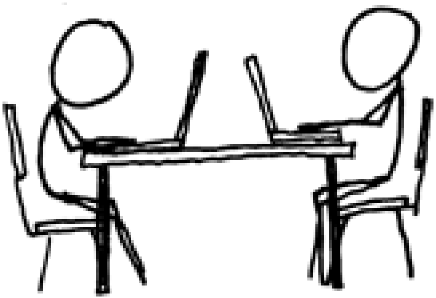

ALICE SENDS A MESSAGE TO BOB SAYING TO MEET HER SOMEWHERE.
UH HUH.
BUT EVE SEES IT, TOO, AND GOES TO THE PLACE.
WITH YOU SO FAR.
BOB IS DELAYED, AND ALICE AND EVE MEET.
YEAH?

I'VE DISCOVERED A WAY TO GET COMPUTER SCIENTISTS TO LISTEN TO ANY BORING STORY.

We are going to talk about all the ways crypto fails us
(and why we still try)

Journalist task: Confidential communication with sources

Step #1: Alice and Bob install crypto software.

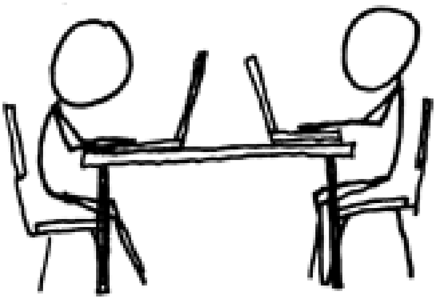


XKCD

The First Date Problem

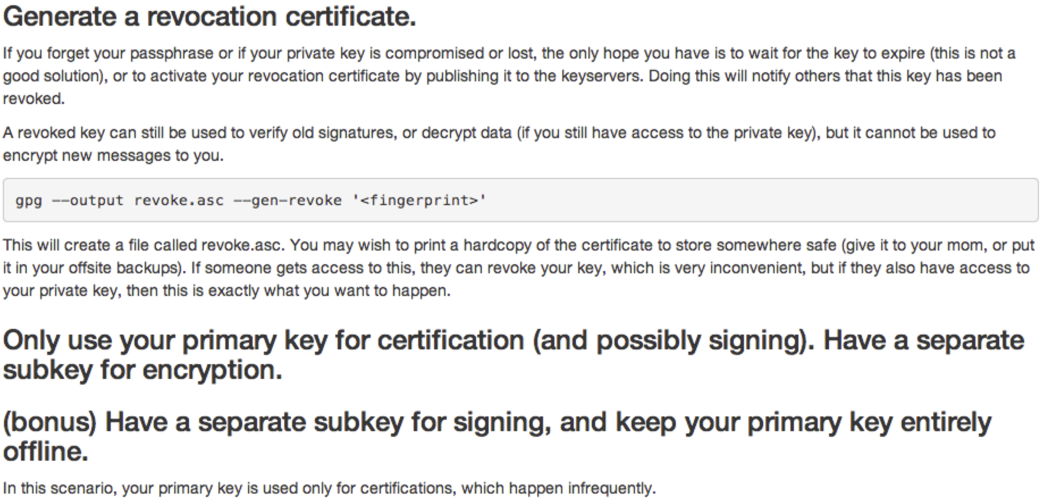
Journalist task: Confidential communication with sources

Step #2: Alice and Bob exchange public keys.



XKCD

The Key Management Problem



Generate a revocation certificate.

If you forget your passphrase or if your private key is compromised or lost, the only hope you have is to wait for the key to expire (this is not a good solution), or to activate your revocation certificate by publishing it to the keyservers. Doing this will notify others that this key has been revoked.

A revoked key can still be used to verify old signatures, or decrypt data (if you still have access to the private key), but it cannot be used to encrypt new messages to you.

```
gpg --output revoke.asc --gen-revoke '<fingerprint>'
```

This will create a file called revoke.asc. You may wish to print a hardcopy of the certificate to store somewhere safe (give it to your mom, or put it in your offsite backups). If someone gets access to this, they can revoke your key, which is very inconvenient, but if they also have access to your private key, then this is exactly what you want to happen.

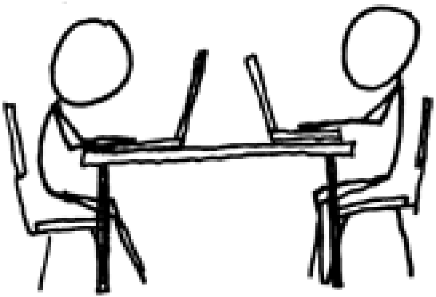
Only use your primary key for certification (and possibly signing). Have a separate subkey for encryption.

(bonus) Have a separate subkey for signing, and keep your primary key entirely offline.

In this scenario, your primary key is used only for certifications, which happen infrequently.

Journalist task: Confidential communication with sources

Step #3: Alice and Bob verify fingerprints.



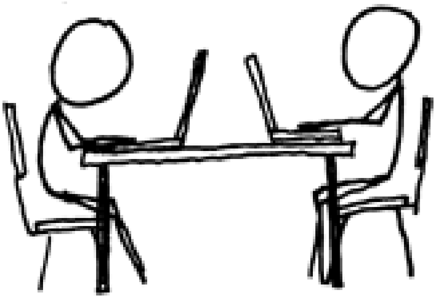
XKCD

The Verification Problem

HEY, I JUST GOT HOME FROM THE PARTY
THE ONE WITH THE IRC FOLKS?
YEAH.
HOW WAS IT?
GOT TOO DRUNK. I SCREWED UP, BAD.
WHAT HAPPENED?
THERE WAS A GIRL. NO IDEA WHO SHE WAS. DON'T EVEN KNOW HER NAME. I WAS TOO DRUNK TO CARE.
AND WHAT, YOU SLEPT WITH HER?
NO.
I SIGNED HER PUBLIC KEY.
SHIT, MAN.

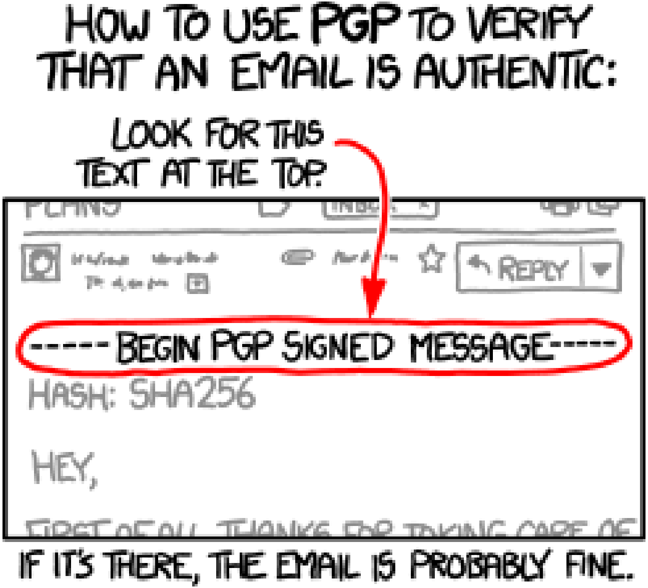
Journalist task: Confidential communication with sources

Step #4: Alice and Bob initiate confidential communication.

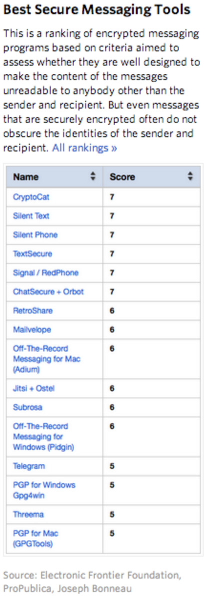


XKCD

The Plaintext Problem


HOW TO USE PGP TO VERIFY THAT AN EMAIL IS AUTHENTIC:
LOOK FOR THIS TEXT AT THE TOP:
PLANS
INBOX
REPLY
-----BEGIN PGP SIGNED MESSAGE-----
HASH: SHA256
HEY,
FIRST OF ALL, THANKS FOR TAKING CARE OF
IF IT'S THERE, THE EMAIL IS PROBABLY FINE.

Hope for the future?



Best Secure Messaging Tools

This is a ranking of encrypted messaging programs based on criteria aimed to assess whether they are well designed to make the content of the messages unreadable to anybody other than the sender and recipient. But even messages that are securely encrypted often do not obscure the identities of the sender and recipient. All rankings »

Name	Score
CryptoCat	7
Silent Text	7
Silent Phone	7
TextSecure	7
Signal / RedPhone	7
ChatSecure + Orbot	7
RetroShare	6
Mailvelope	6
Off-The-Record Messaging for Mac (Adium)	6
Jitsi + Ostel	6
Subrosa	6
Off-The-Record Messaging for Windows (Pidgin)	6
Telegram	5
PGP for Windows Gpg4win	5
Threema	5
PGP for Mac (GPGTools)	5

Source: Electronic Frontier Foundation, ProPublica, Joseph Bonneau

Journalist task: Anonymous communication with sources

Step #1: Alice purchases Bob a burner phone with cash.

Step #2: Alice installs apps and contacts on Bob’s phone.

Step #3: Alice mails Bob his special burner phone.

Step #4: Bob uses his burner phone to securely communicate with Alice.

The Burner Problem

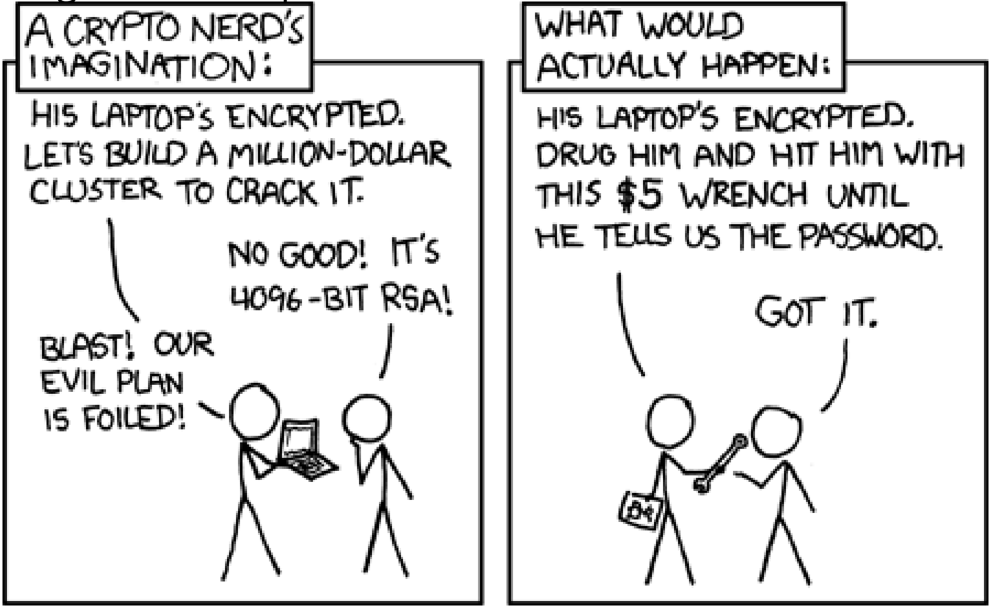
Hope for the future?

Journalist task: Keeping notes and data

Step #1: Alice encrypts her data to her private key.

The collaboration problem

The legal coercion problem



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.
B4

The international border problem

Hope for the future?

Questions? Answers?