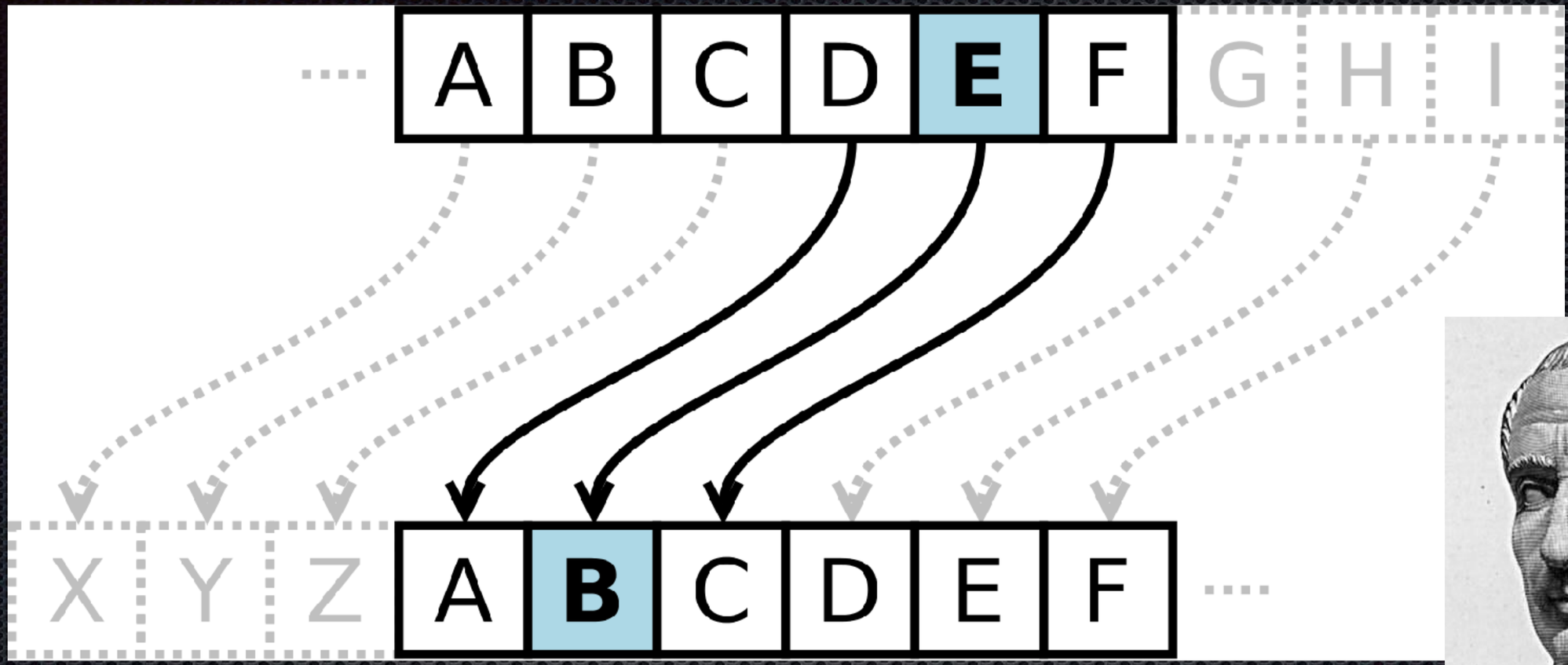
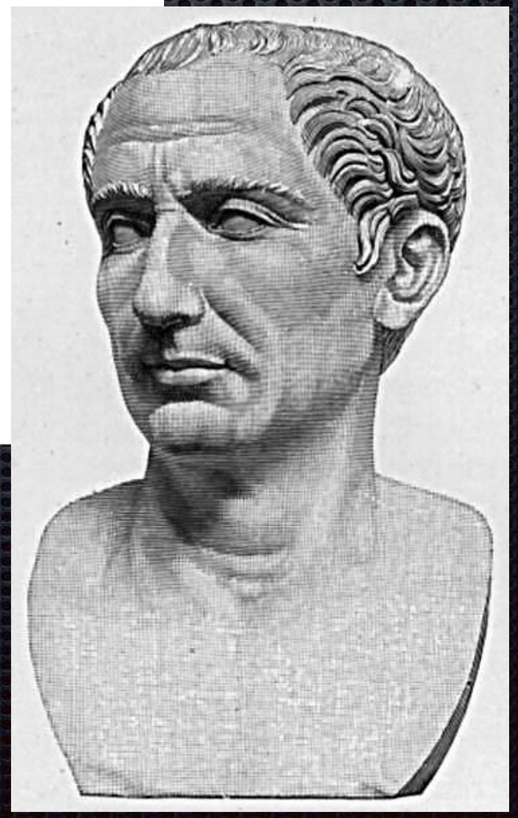
Secure Communication & Data Sharing with PGP

Bankim Tejani

Agenda

- Refresher on encryption basics
- Why protect your data?
- Why PGP?
- How do I use PGP?
- Uses beyond secure e-mail


A B C D E F G H I
X Y Z A B C D E F

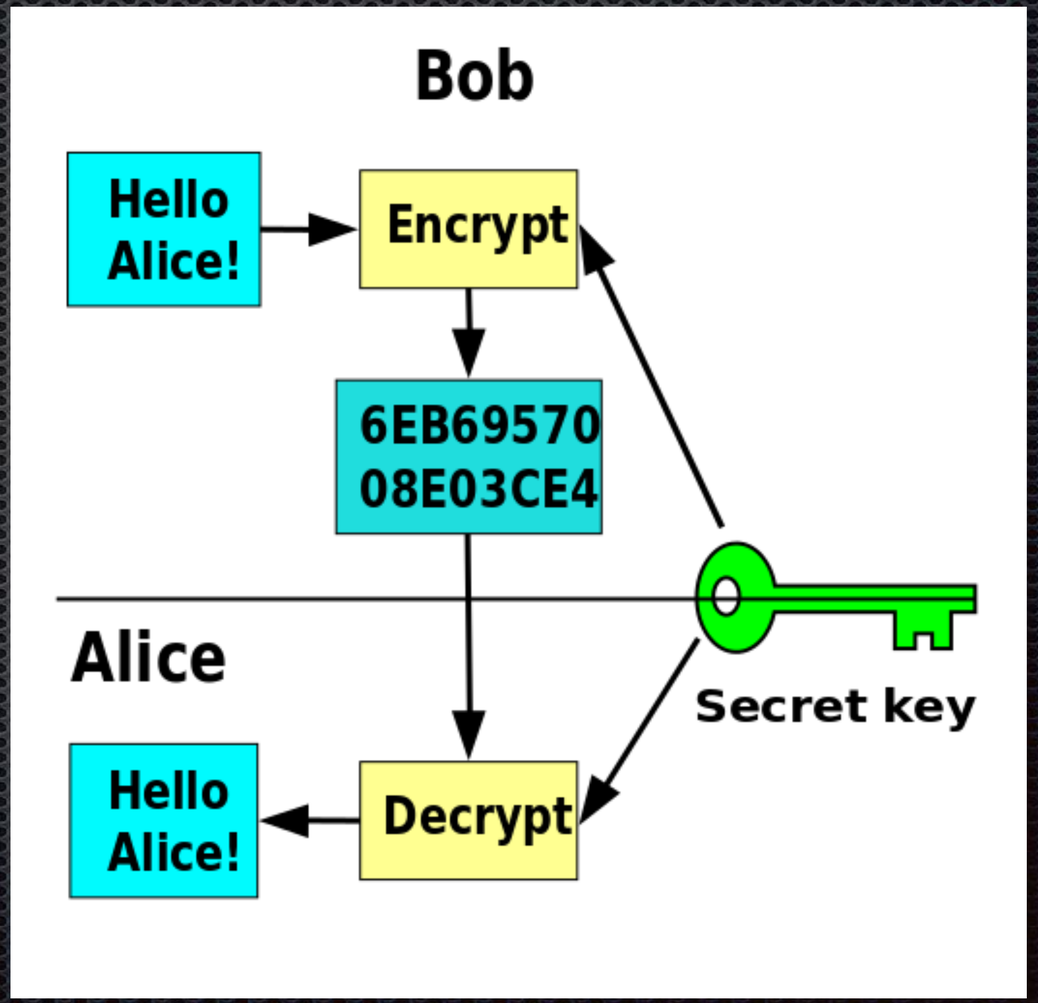



THE CIPHER MACHINE
ENIGMA
THE PRE WAR YEARS 1923 - 1939
Commercial ENIGMA
"G" ENIGMA


THE CIPHER MACHINE
ENIGMA
THE WAR YEARS 1939 - 1945

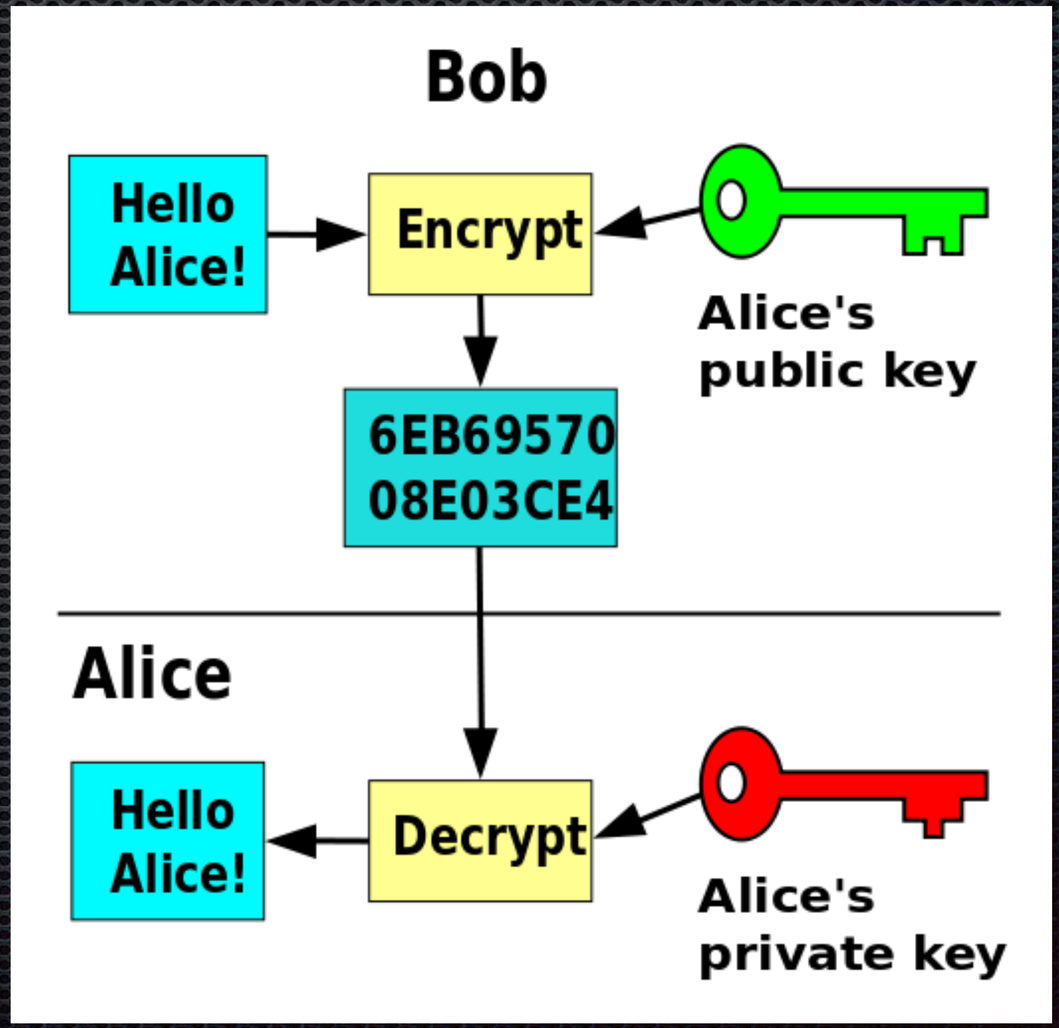
Symmetric Encryption

- Typically private key or shared key
- Fast, efficient
- Only as secure as the key
- DES, 3DES, AES, Camellia



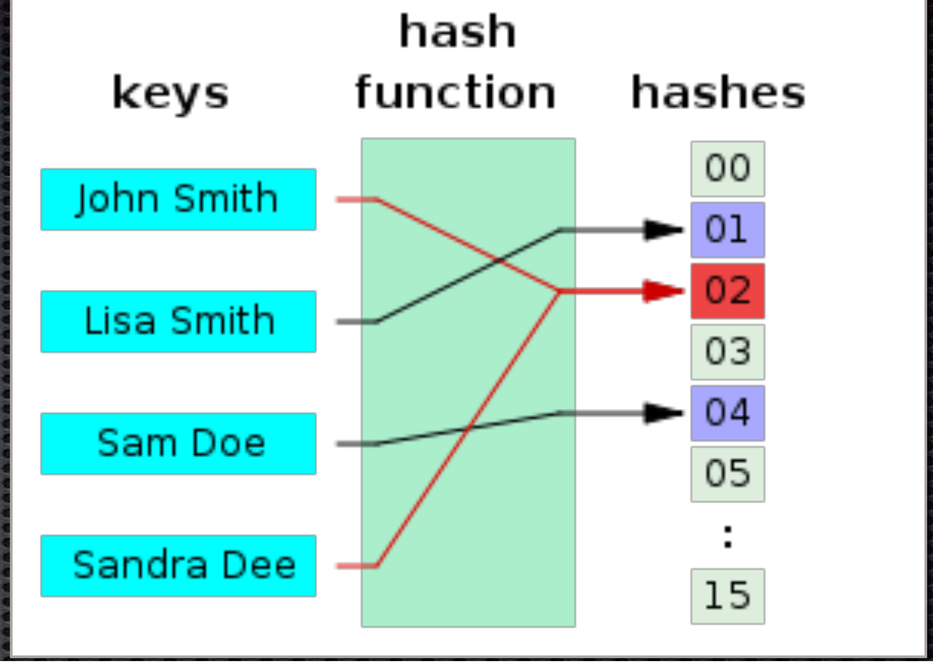
Asymmetric Encryption

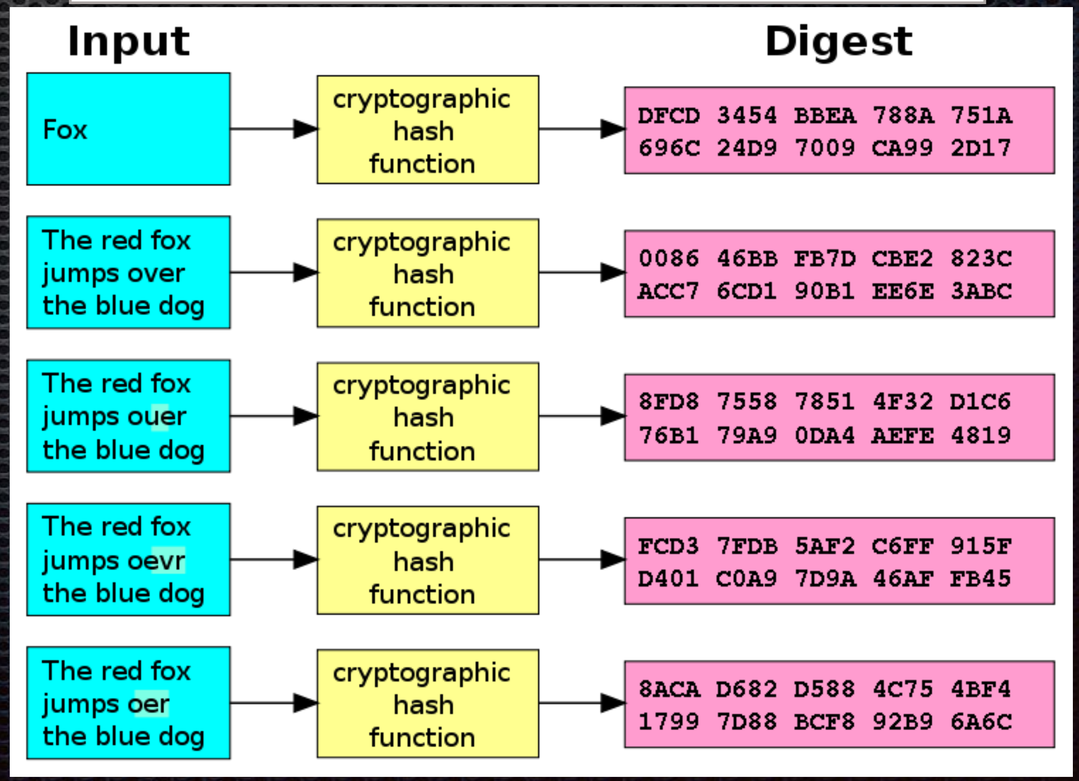
- a.k.a. Public Key or Public/ Private key pair encryption
- Trust & authentication
  - Certificate Authority
- Only as secure as private key
- RSA, PGP



Hashing

- One-way function
- Deterministic & efficient
- Small change to input creates dramatic entropy in output
- Fantastic for checksums
- MD5, SHA, MACs, signatures





Protect Your Data

- Data privacy laws - GDPR
- Privacy policy / Terms of Service
- Employment agreement
- PCI, SOX, other
- Its your data too!
- Don’t be evil…

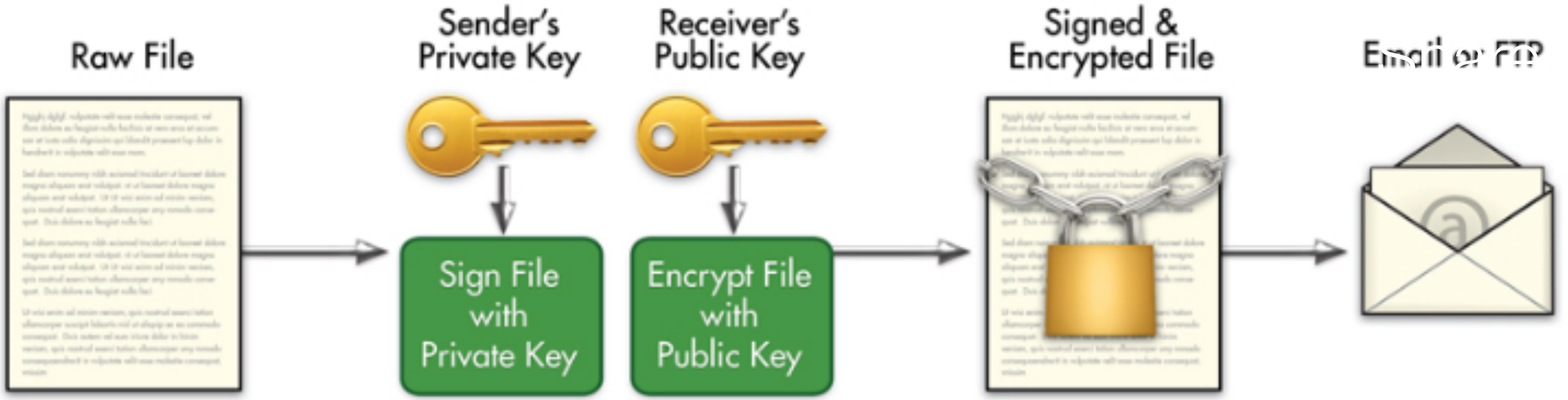
Pretty Good Privacy (PGP)

- Developed 1991, P. Zimmerman
- Survived lawsuits, sanctions, corporate takeovers, and t-shirts
- “the closest you're likely to get to military-grade encryption.”
  -Bruce Schneier
- Free!

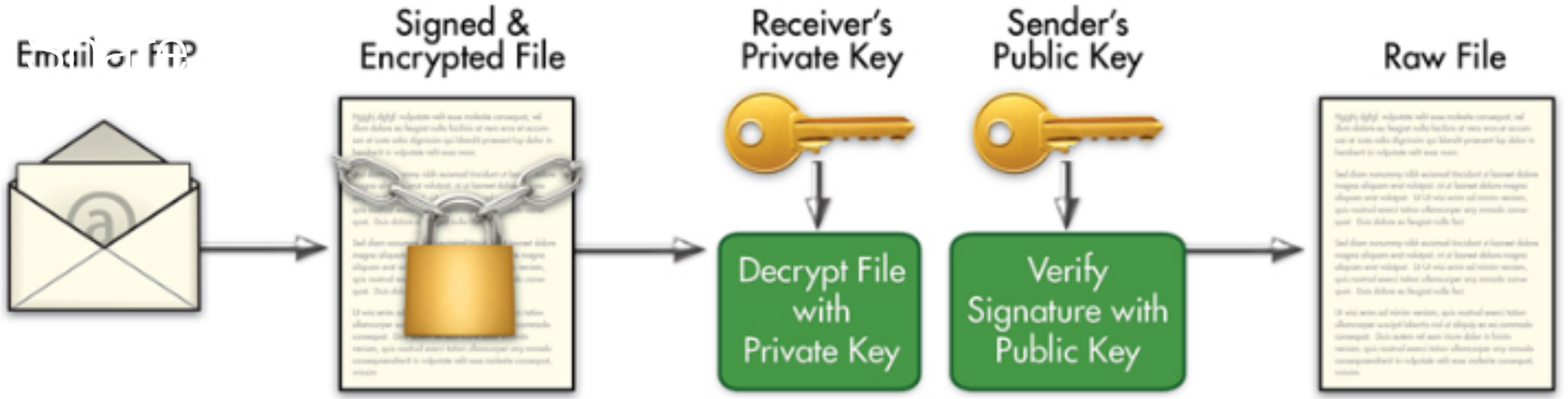
Pretty Good Privacy (PGP)

- Asymmetric cryptography
- Hash-based signatures
- Public key repositories
- Web of trust

Sender | Signing & Encryption Process



Receiver | Decryption & Verification Process

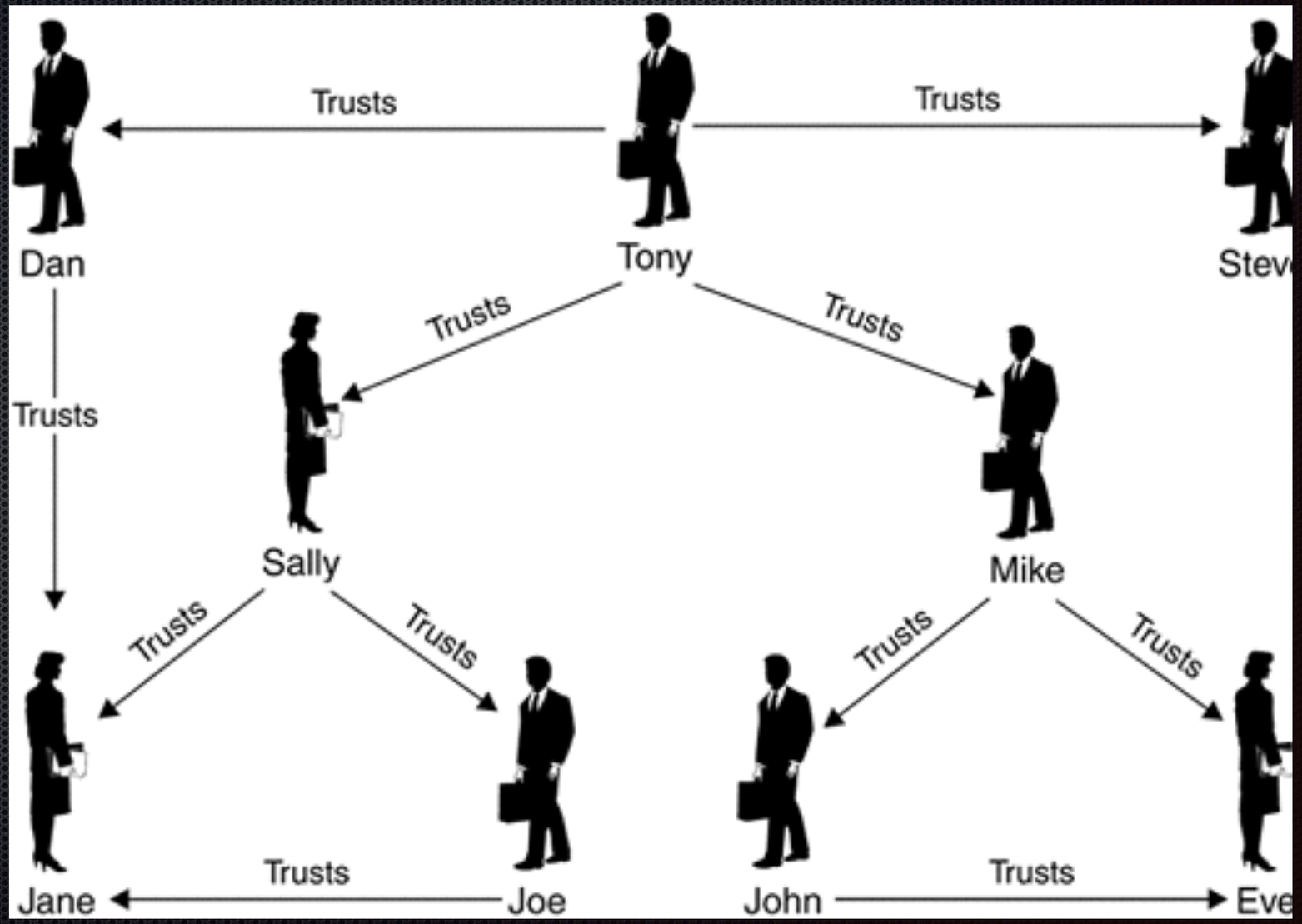


Using PGP

- Get software
- Generate your keys
- Share & download public keys
- Encrypt & sign
- Decrypt & verify
- Share

Web of Trust

- Trust through network
- Sign others' public keys to indicate trust
- Shared publicly via keyservers

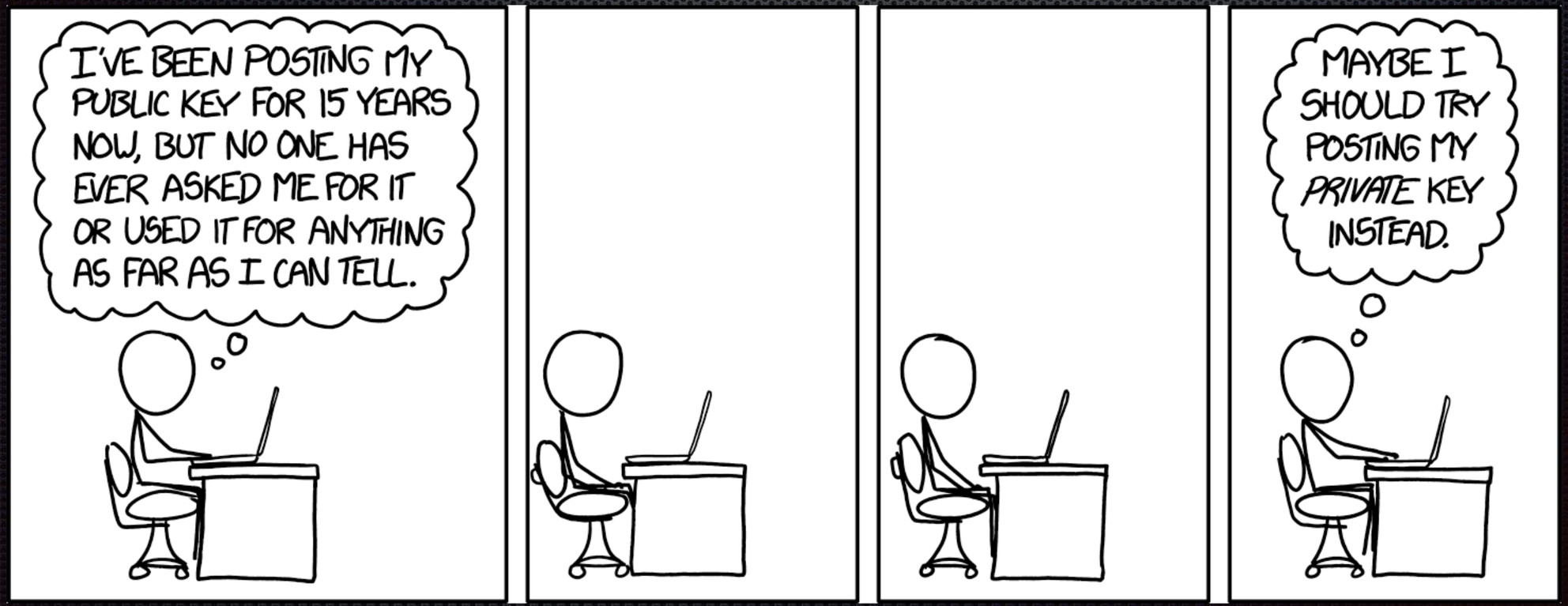



HEY, I JUST GOT HOME FROM THE PARTY
THE ONE WITH THE IRC FOLKS?
YEAH.
HOW WAS IT?
GOT TOO DRUNK. I SCREWED UP, BAD.
WHAT HAPPENED?
THERE WAS A GIRL. NO IDEA WHO SHE WAS. DON'T EVEN KNOW HER NAME. I WAS TOO DRUNK TO CARE.
AND WHAT, YOU SLEPT WITH HER?
NO.
I SIGNED HER PUBLIC KEY.
SHIT, MAN.

Innovative Uses

- Data pipelines
- Data sharing w/ partners
- Report / data protection
- Log protection / integrity
- Disk Images

Questions?


I'VE BEEN POSTING MY PUBLIC KEY FOR 15 YEARS NOW, BUT NO ONE HAS EVER ASKED ME FOR IT OR USED IT FOR ANYTHING AS FAR AS I CAN TELL.
MAYBE I SHOULD TRY POSTING MY PRIVATE KEY INSTEAD.