Everything you need to know about Cryptography

(unless you're a mathematician)

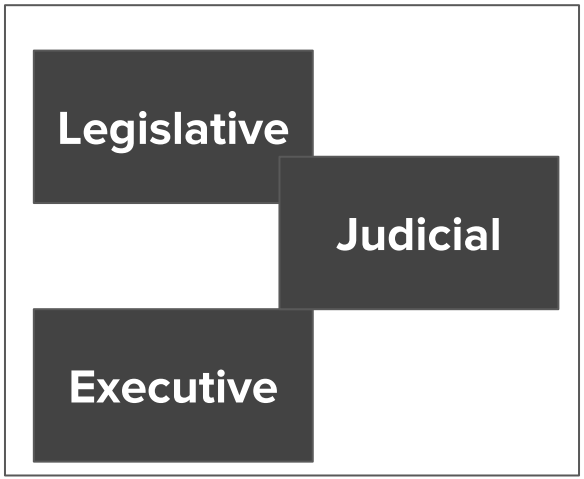
Black Boxes

Black Boxes

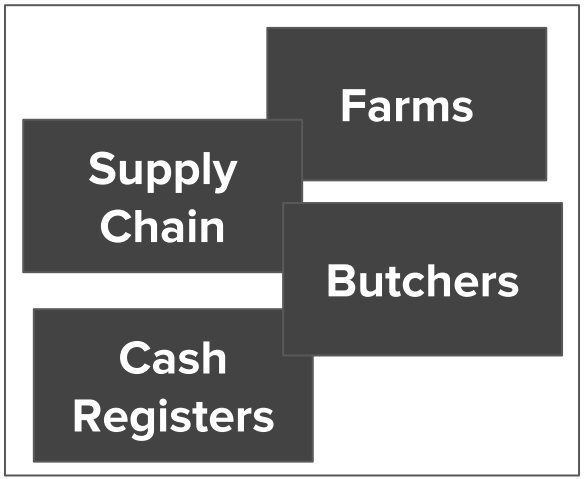
Black Boxes

Black Boxes

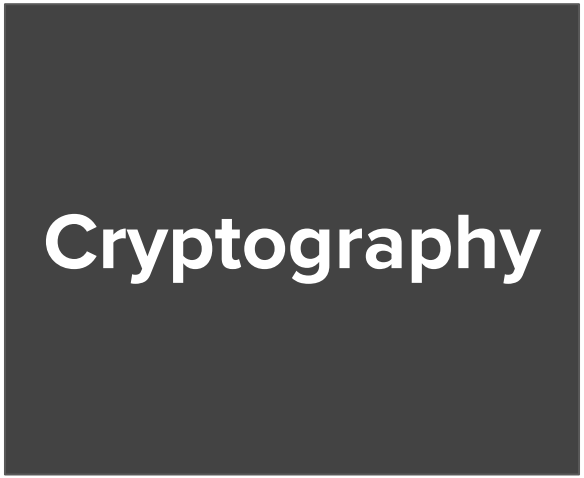
Government



Grocery Store

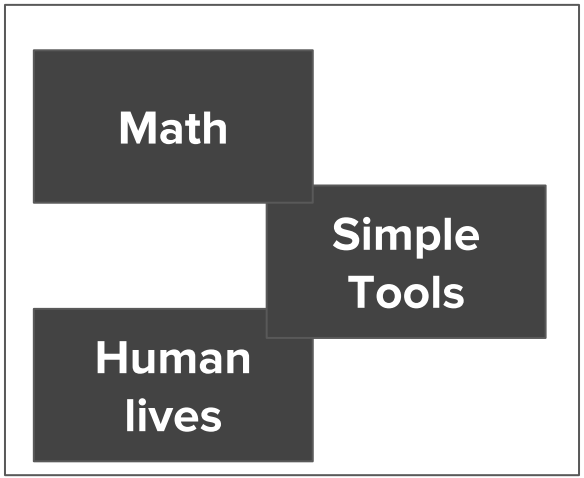


Black Boxes



Black Boxes

Cryptography



Basic Cryptographic Tools

Don’t try this at home.

Get an expert.

Basic Cryptographic Tools

Seriously though. Bad crypto ruins lives.

Basic Cryptographic Tools

Primitive machines

Randomness

Actively Used

- Keystrokes
- Cosmic Microwave Background
- Dice

Broken

- Humans

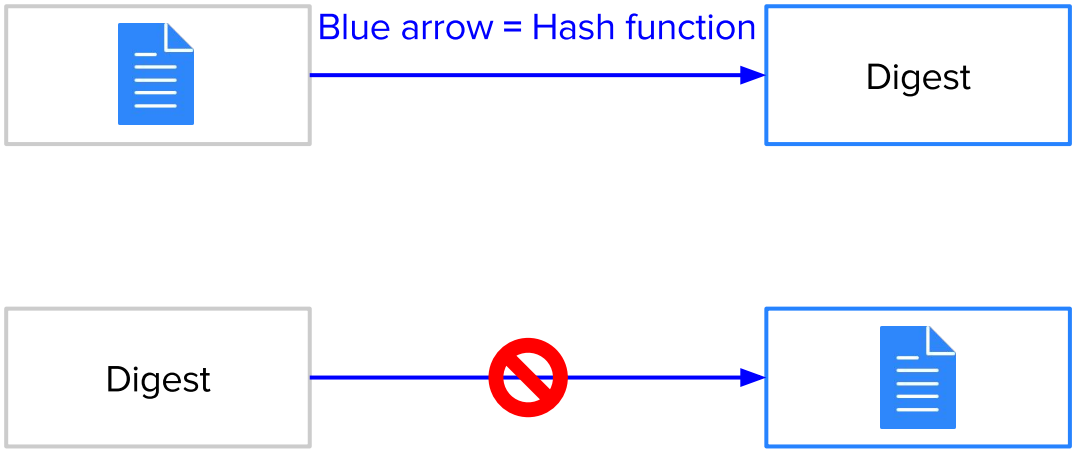
Actively Used

- Hash functions
- Block ciphers
- Really hard math

Backdoored

- Dual EC DRBG

Cryptographic Hash Functions



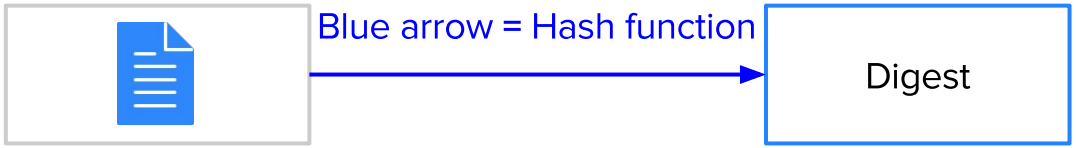
Properties of Hash Functions

What goes in

- Data

What comes out

- A unique label



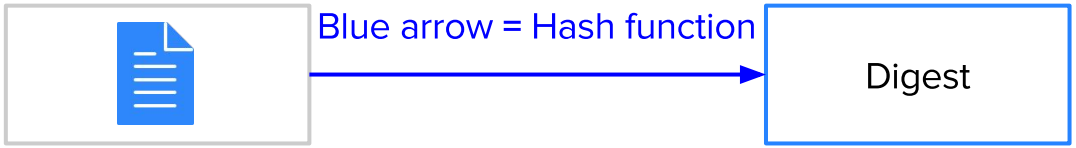
Important Properties

- Irreversible
- Collision-free
- Unpredictable
- Deterministic

Common Hash Functions

Actively Used

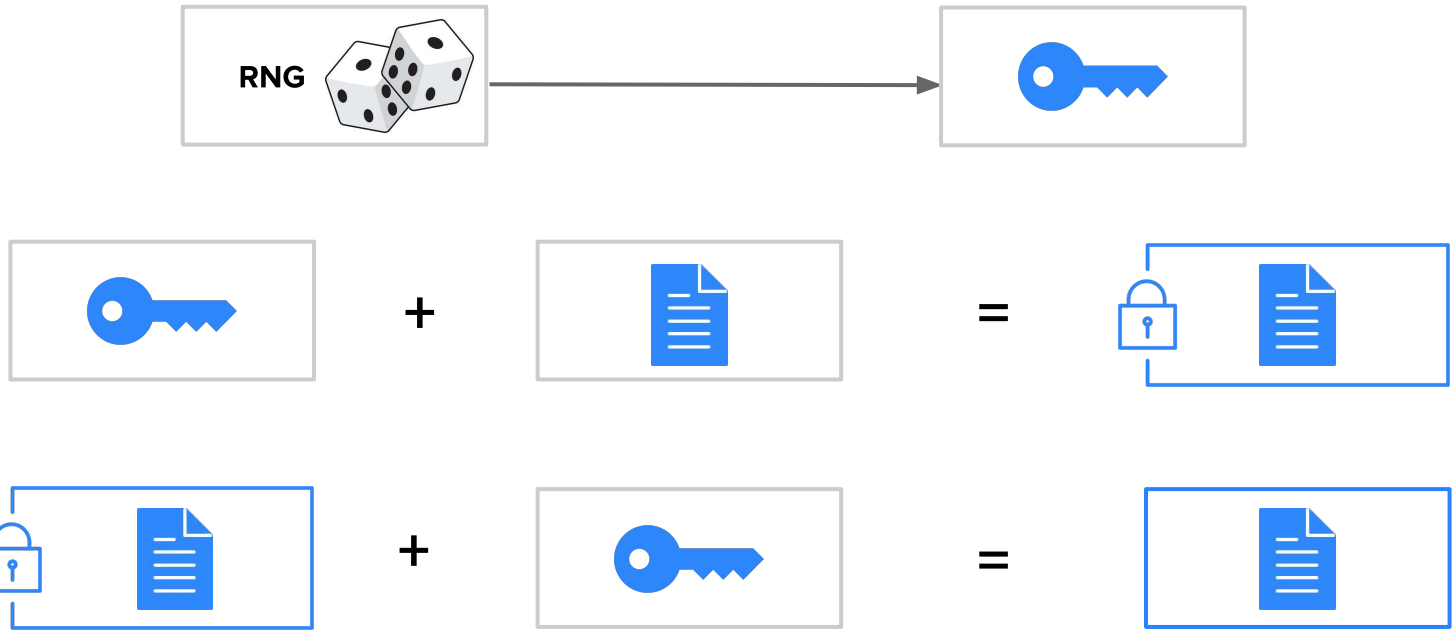
- SHA2 (256 or 512)
- SHA3 / Keccak
- Blake2
- Ripemd160



Broken

- SHA1
- md5

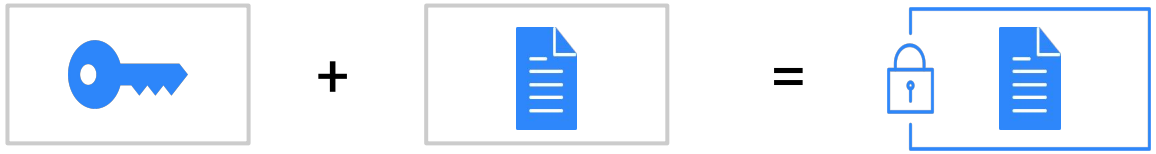
Symmetric Encryption



Properties of Symmetric Encryption Algorithms

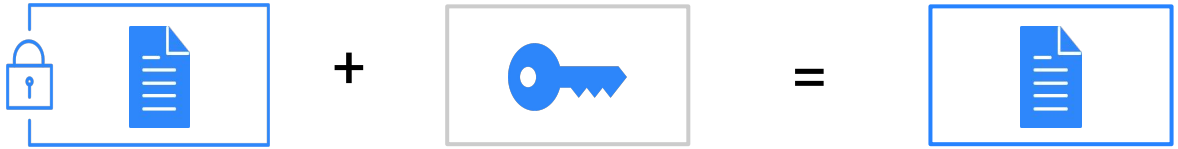
What goes in

- A message
- A key



What comes out

- Ciphertext



Important properties

- Fast AF
- Reversible (with the key)
- You have to transmit a secret :(

Completely unrelated issues will ruin your crypto

Common Symmetric Encryption Algorithms

Actively Used

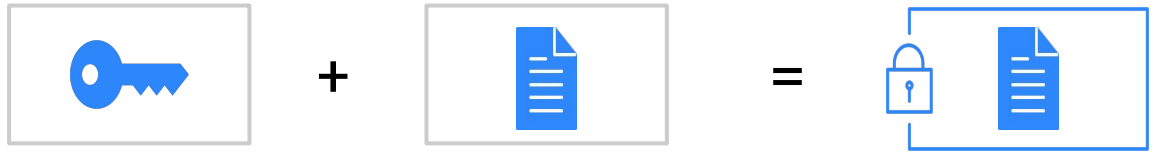
- AES
- 3DES

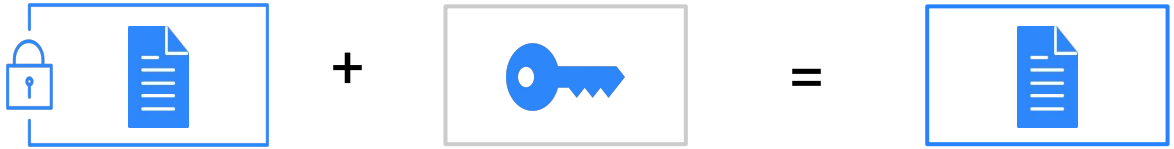
Broken

- DES
- RC4

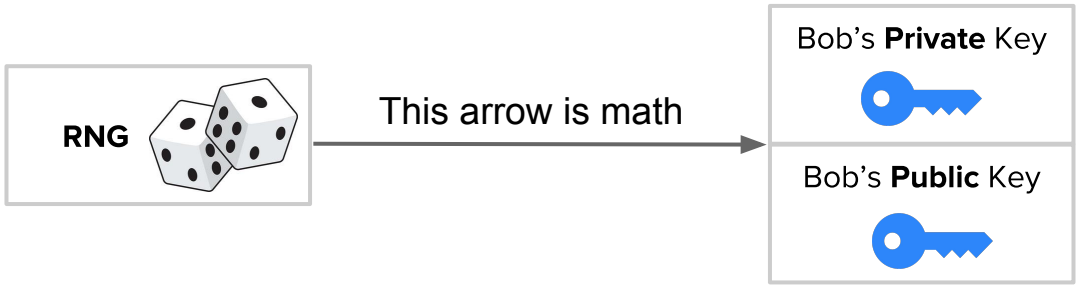
Backdoored

- Skipjack

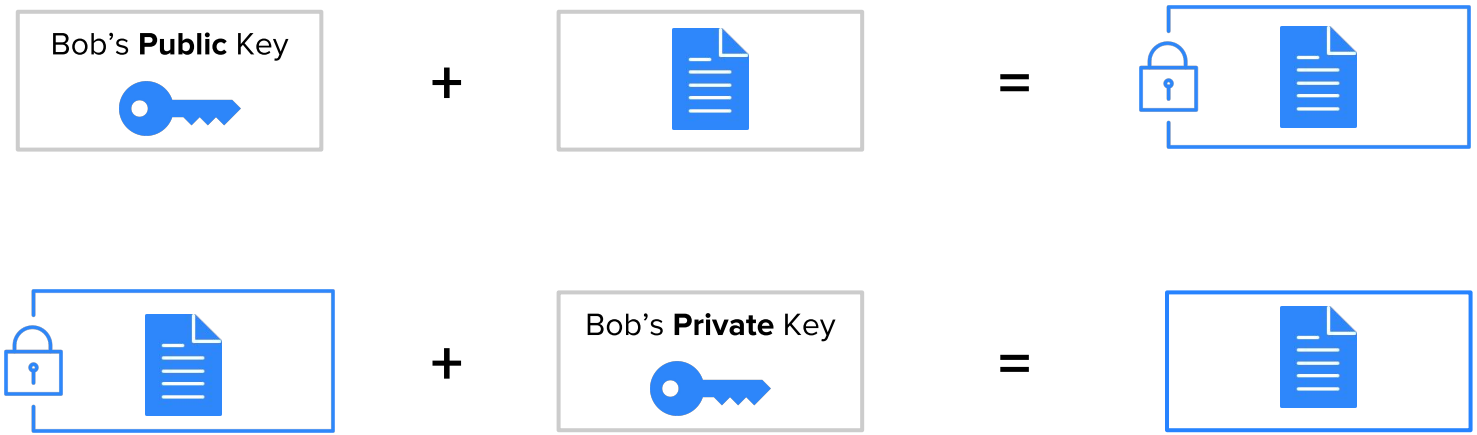




Public-key Cryptography



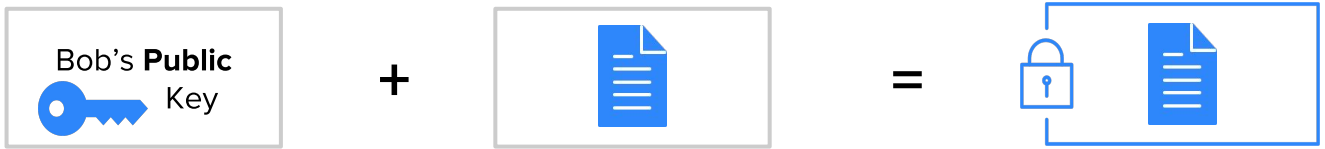
Public-key Cryptography - Asymmetric Encryption



Properties of Asymmetric Encryption Algorithms

What goes in

- A message
- A keypair



What comes out

- Ciphertext

Important properties

- Really really slow
- No secrets are sent

Public Key Cryptography - Signing

Properties of Digital Signature Algorithms

What goes in

- A message
- A keypair

What comes out

- A digital signature

Important properties

- Pretty slow
- Can’t be forged
- Can’t be denied

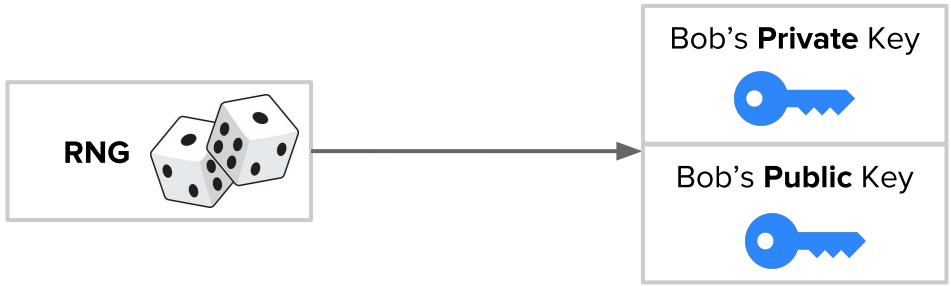
Common Public-Key Cryptography Algorithms

Actively Used

- RSA
- ECDSA
- EdDSA

Maybe Soon

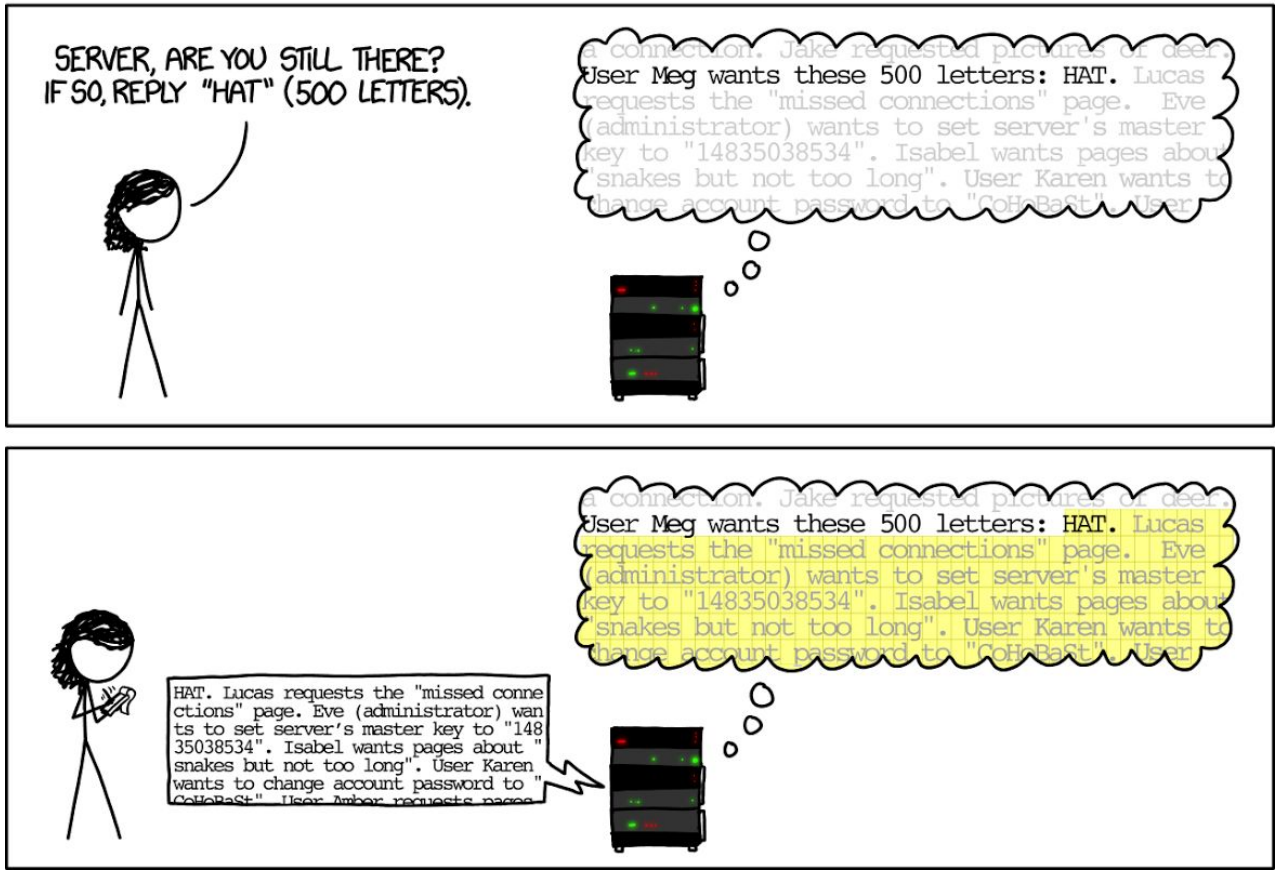
- BLS Short signatures
- Schnorr
- Threshold signatures



Cryptosystems

Cryptographic tools are hard enough to make

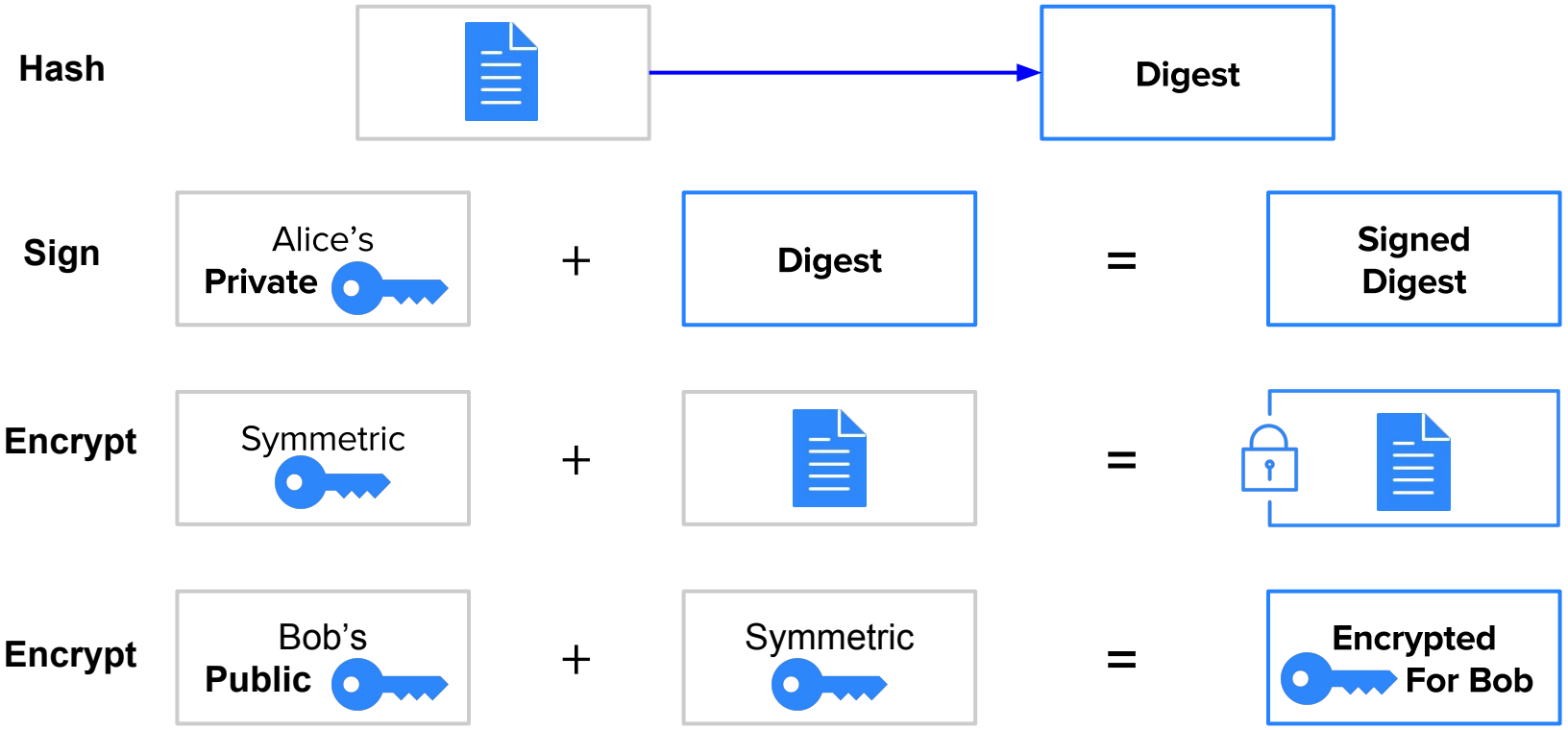
But even the plumbing is dangerous


SERVER, ARE YOU STILL THERE? IF SO, REPLY "HAT" (500 LETTERS).
User Meg wants these 500 letters: HAT.
HAT. Lucas requests the "missed conne ctions" page. Eve (administrator) wan ts to set server's master key to "148 35038534". Isabel wants pages about " snakes but not too long". User Karen wants to change account password to "

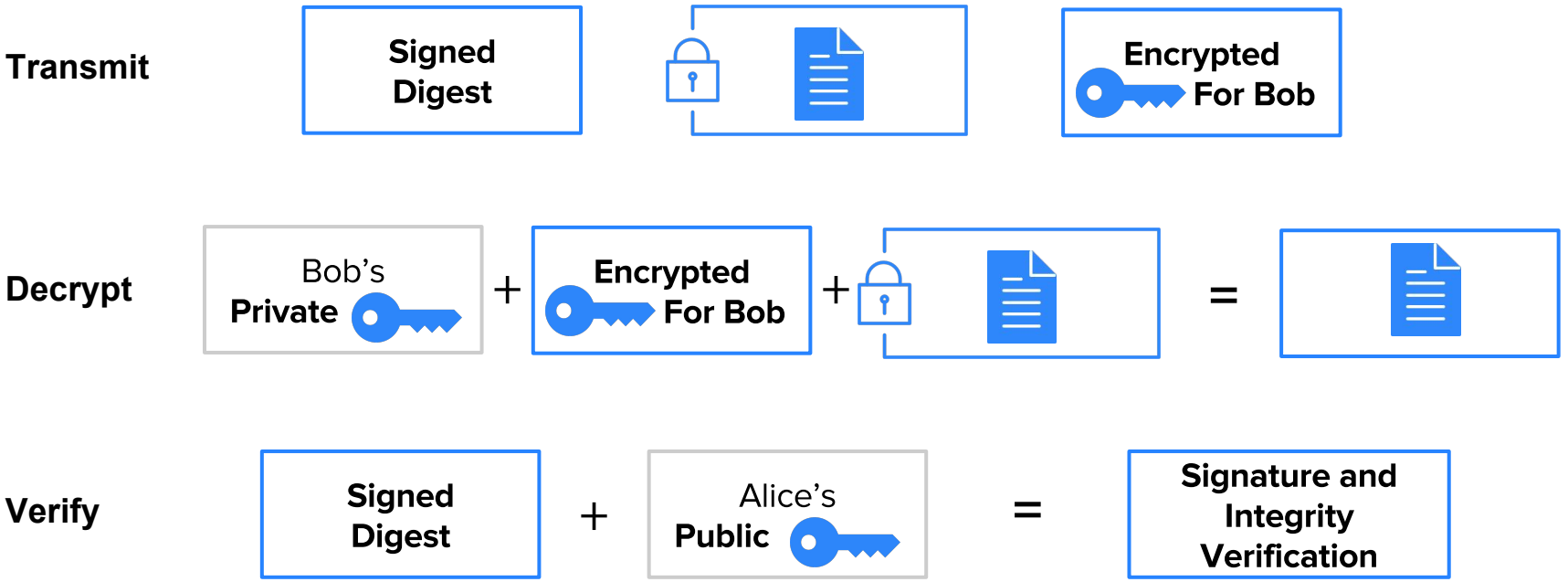
Cryptosystems

AKA ultra-high-stakes plumbing

PGP - Part 1

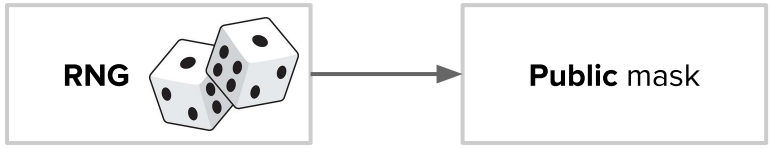

Hash
Digest
Sign
Alice's
Private
+
Digest
=
Signed
Digest
Encrypt
Symmetric
+
=
Encrypt
Bob's
Public
+
Symmetric
=
Encrypted
For Bob

PGP - Part 2


Transmit
Signed Digest
Encrypted For Bob
Decrypt
Bob's Private
+
Encrypted For Bob
+
=
Verify
Signed Digest
+
Alice's Public
=
Signature and Integrity Verification

Diffie-Hellman Key Exchange - Part 1

Generate



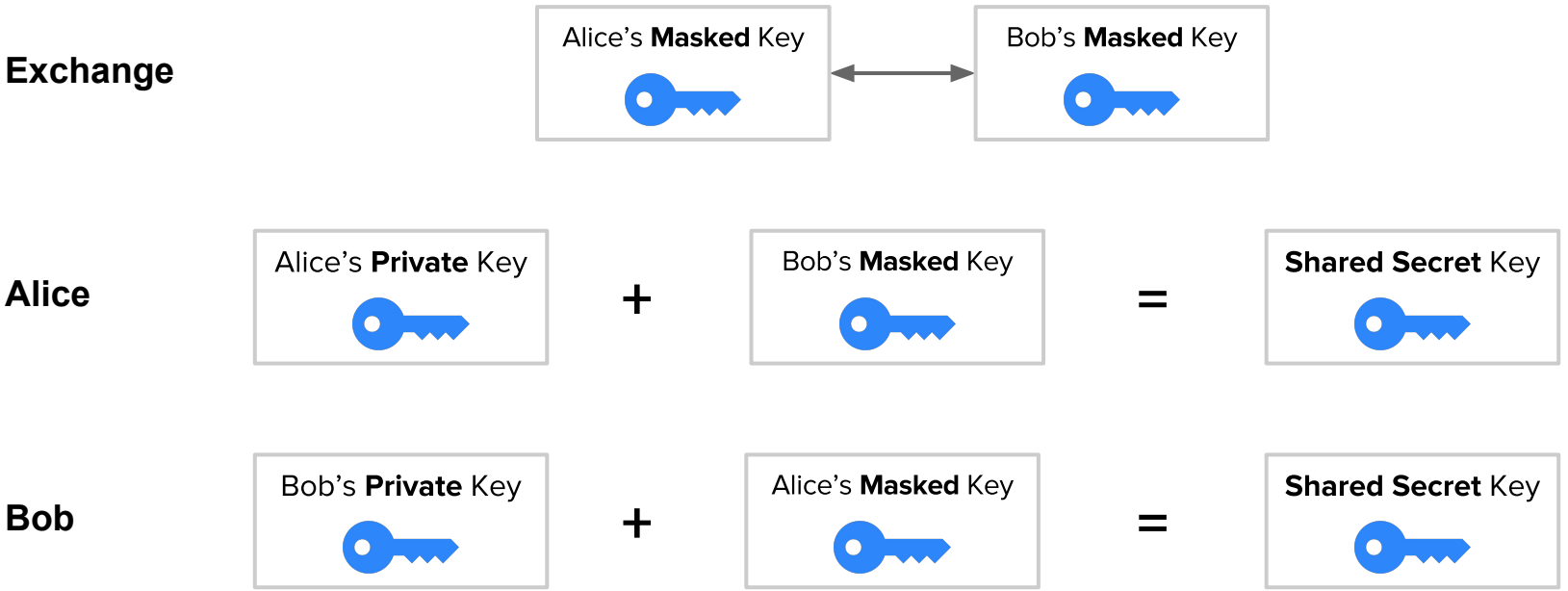
Alice

Alice's **Private** Key + **Public** mask = Alice's **Masked** Key

Bob

Bob's **Private** Key + **Public** mask = Bob's **Masked** Key

Diffie-Hellman Key Exchange - Part 2



Properties of D-H

What goes in

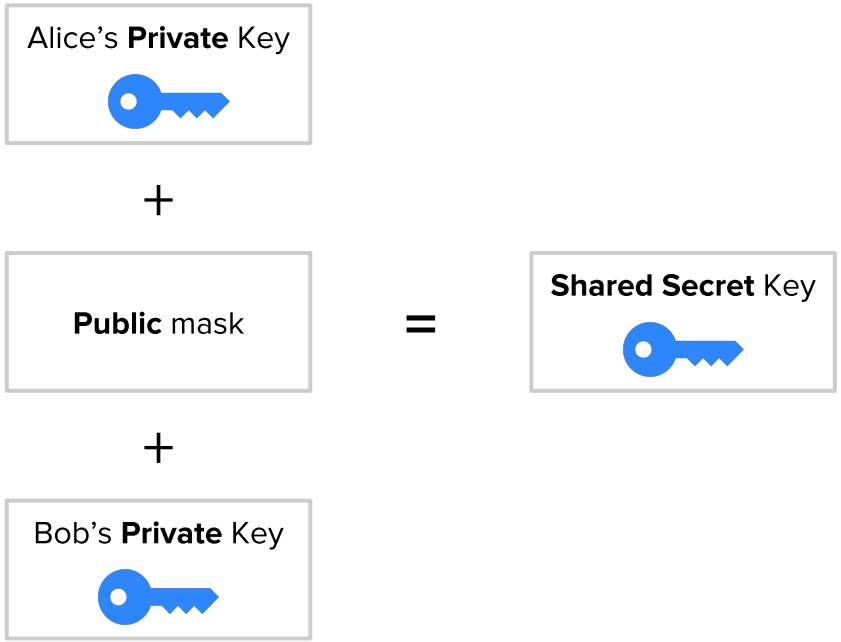
- A shared public mask
- Bob and Alice's secret keys

What comes out

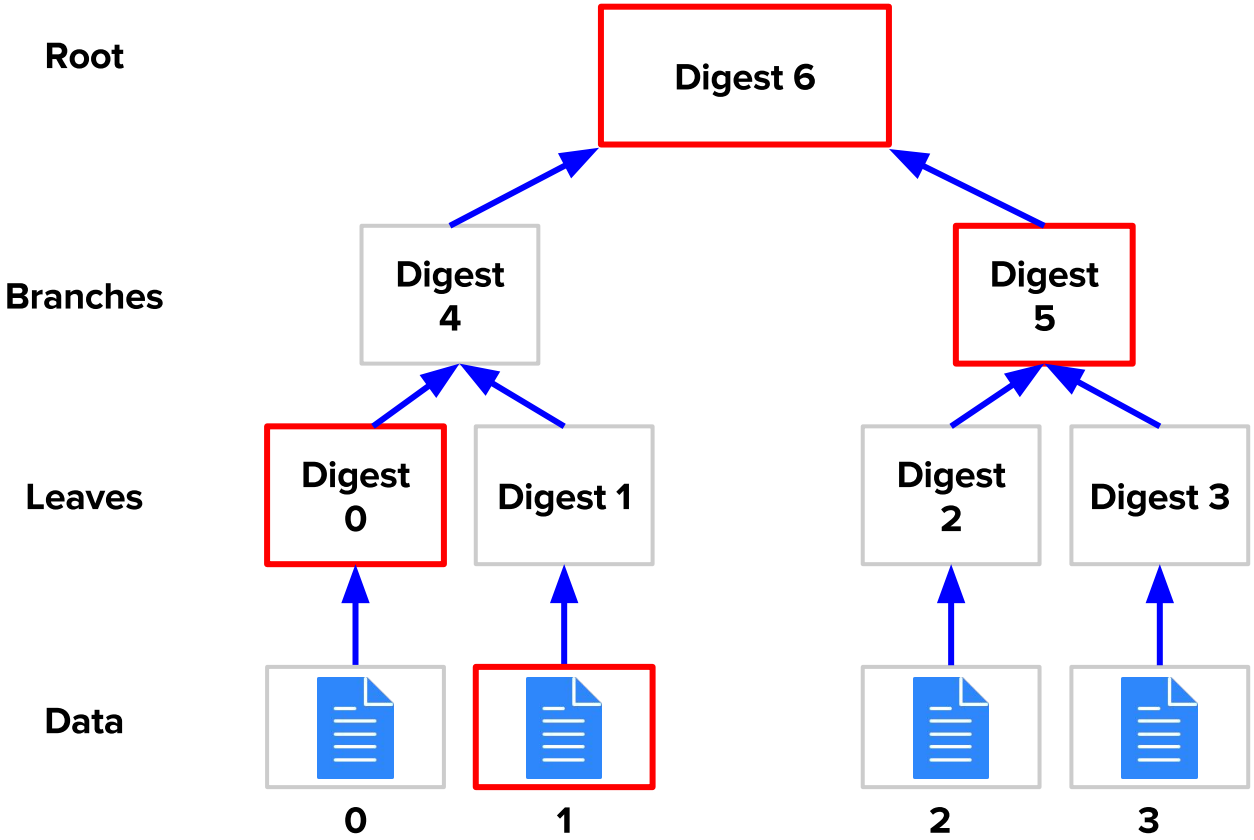
- A shared secret key

Important properties

- No key leakage
- No eavesdropping



Merkle Tree


Root
Digest 6
Branches
Digest 4
Digest 5
Leaves
Digest 0
Digest 1
Digest 2
Digest 3
Data
0
1
2
3

Properties of a Merkle Tree

What goes in

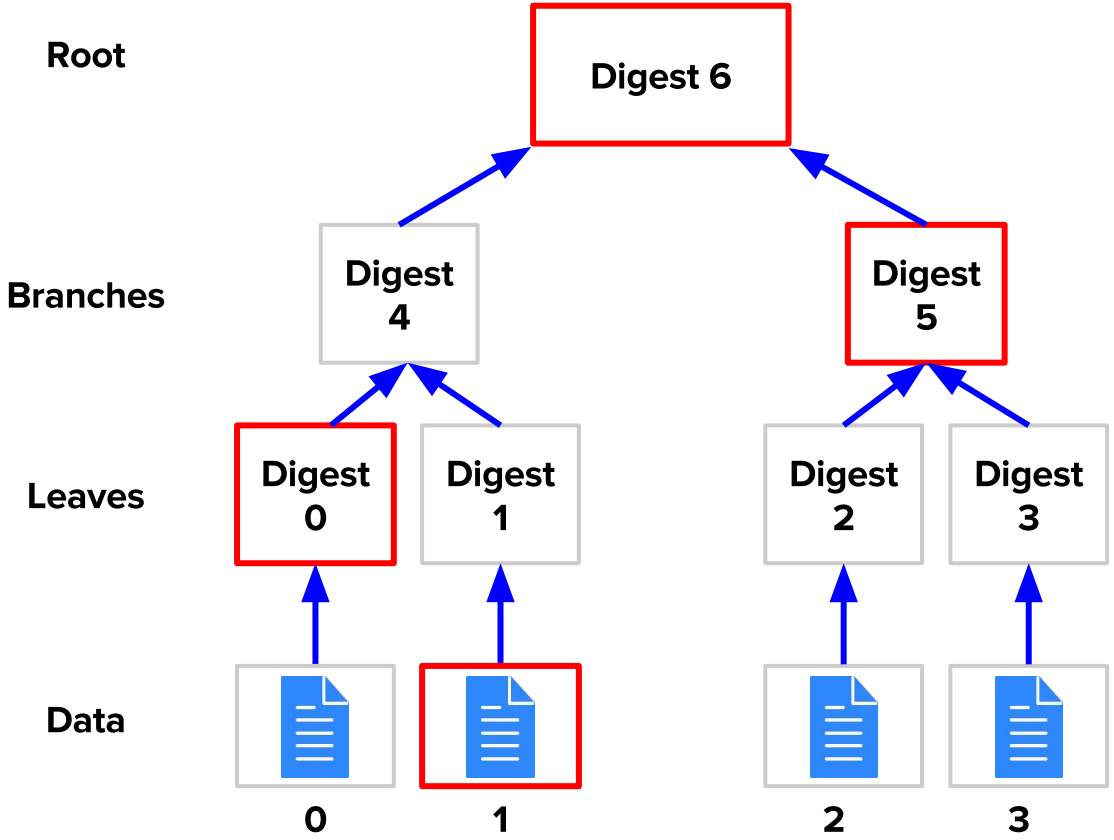
- Data

What comes out

- A tree of hashes

Important properties

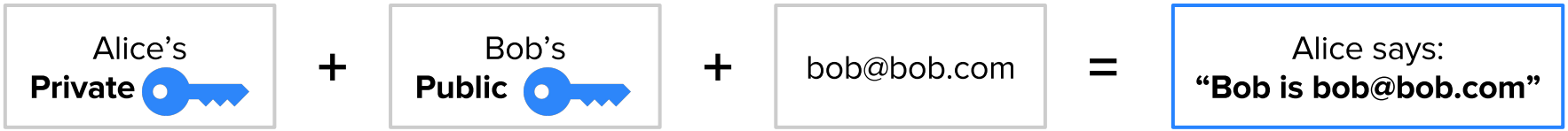
- Prove presence of any data
- Prove integrity of any data
- Prove integrity of whole



Identity & Trust

Who is this Bob guy anyway?

PGP Web of Trust



Properties of PGP Web of Trust

What goes in

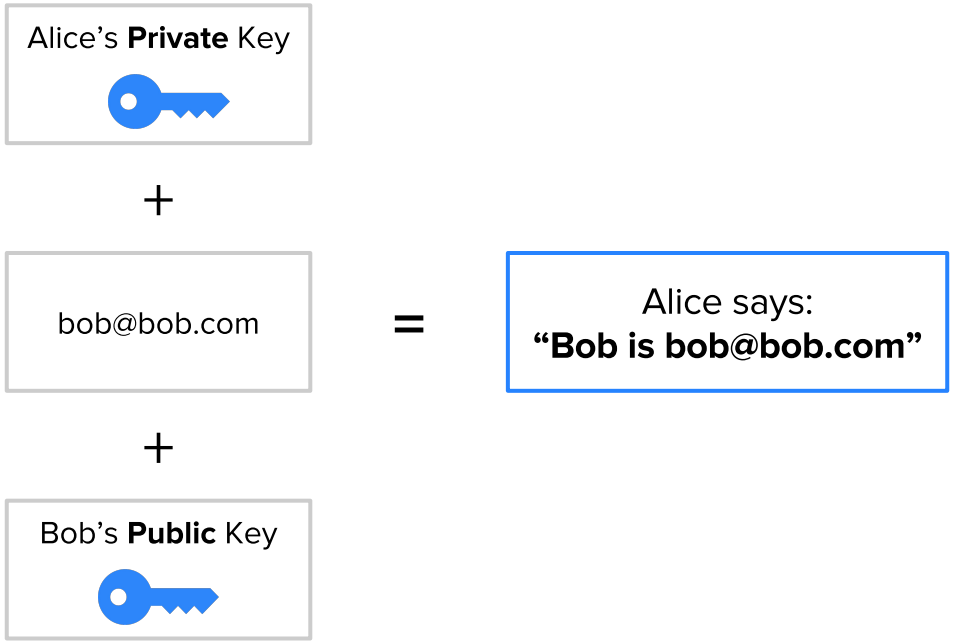
- Keypairs

What comes out

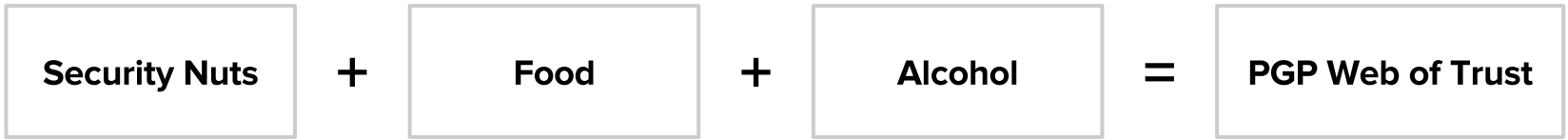
- Signed public keys

Important properties

- Transitive trust
- Limited lifespan
- Subjectivity



Key-signing Parties



Properties of Key Signing Parties

What goes in

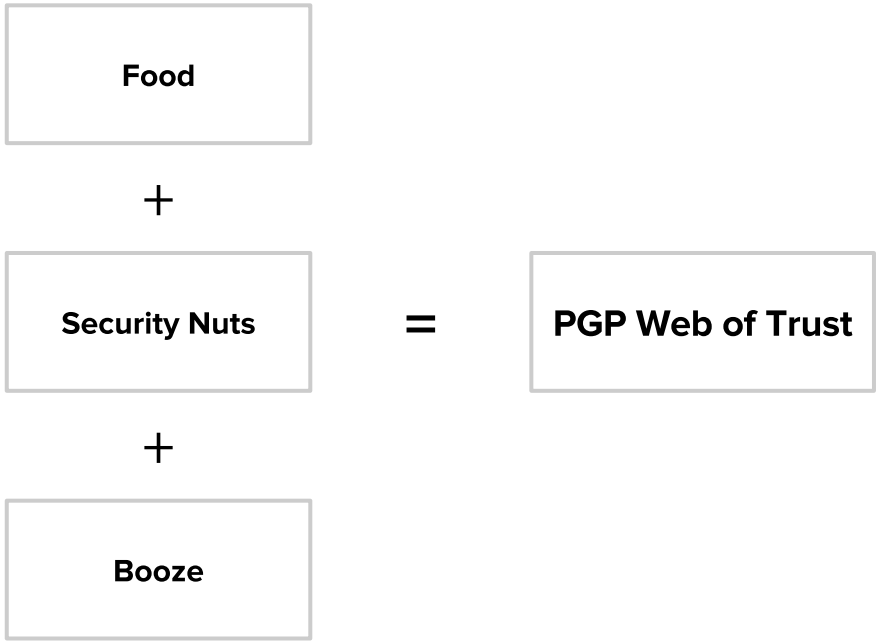
- A shared public mask
- Bob and Alice's secret keys

What comes out

- A bunch of signed keys

Important properties

- Sometimes awkward
-



TLS Certificates (X.509)

Properties of Certificates (X.509)

What goes in

- A trusted authority
- A name and a pubkey

What comes out

- An identity certificate

Important properties

- The foundation of HTTPS
- Relies on known authorities