DS 593: Privacy in Practice

High Level Introduction to Cryptography

Instructor: Alishah Chator

News?

Your email and social media account can be accessed by income tax officers starting next financial year in these cases

By Ira Alok Puranik, ET Online • Last Updated: Mar 04, 2025, 11:14:00 AM IST

FOLLOW US SHARE FONT SIZE SAVE PRINT COMMENT 10

https://economictimes.indiatimes.com/wealth/tax/your-email-and-social-media-account-can-be-accessed-by-income-tax-officer-starting-next-financial-year-in-these-cases/articleshow/118685184.cms

Last time

- The Internet!

Today

- What is Cryptography

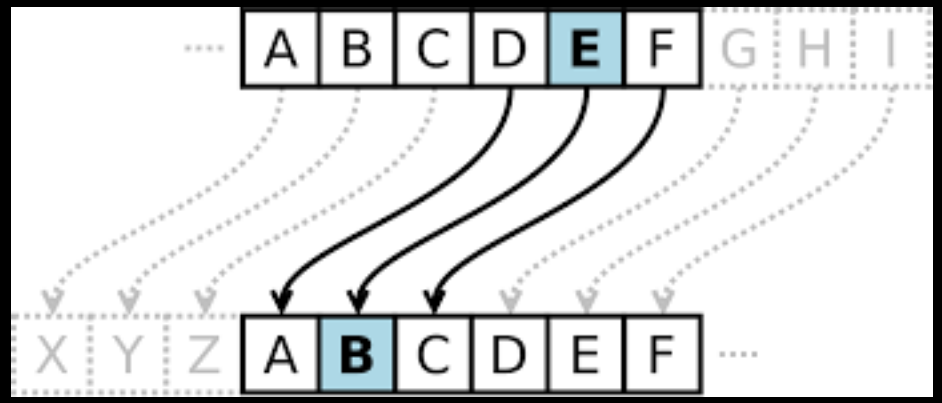
Goals

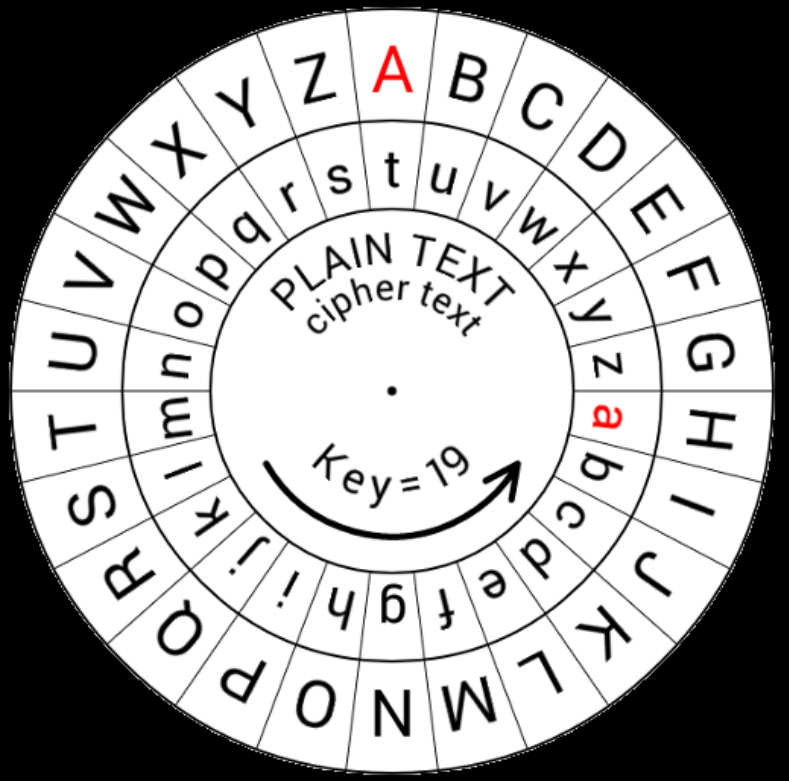
- Build an intuition of the various cryptographic tools we have at our disposal for building privacy enhancing technologies (PETs)
- This is not a cryptography course, we will not be going into the weeds of constructions and proofs

What does cryptography mean to you?

Cryptography

- Literally means the writing of secret messages
- For most of its history, this is all it was!


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


A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
a b c d e f g h i j k l m n o p q r s t u v w x y z
PLAIN TEXT
cipher text
Key=19

Cryptography

- More generally, cryptography is the *study* and *practice* of *secure communication* in the presence of *adversarial behavarior*

Cryptography

- More generally, cryptography is the *study* and *practice* of *secure communication* in the presence of *adversarial behavarior*

- Secrecy is part of this

- So is authenticity and identity

- In many ways it is about trust

Security in Cryptography

- Its about secret information *not* secret algorithms
  - At least in theory
- Security through Obscurity
  - Not what we want
- Ideally, we minimize what has to be kept secret

Kerckhoff’s Principle

1. The system must be practically, if not mathematically, indecipherable;

2. ***It should not require secrecy, and it should not be a problem if it falls into enemy hands;***

3. It must be possible to communicate and remember the key without using written notes, and correspondents must be able to change or modify it at will;

4. It must be applicable to telegraph communications;

5. It must be portable, and should not require several persons to handle or operate;

6. Lastly, given the circumstances in which it is to be used, the system must be easy to use and should not be stressful to use or require its users to know and comply with a long list of rules.

Plaintext

A Study in Scarlet — Edited

CHAPTER II.
THE SCIENCE OF DEDUCTION.

We met next day as he had arranged, and inspected the rooms at No. 221B, Baker Street, of which he had spoken at our meeting. They consisted of a couple of comfortable bed-rooms and a single large airy sitting-room, cheerfully furnished, and illuminated by two broad windows. So desirable in every way were the apartments, and so moderate did the terms seem when divided between us, that the bargain was concluded upon the spot, and we at once entered into possession. That very evening I moved my things round from the hotel, and on the following morning Sherlock Holmes followed me with several boxes and portmanteaus. For a day or two we were busily employed in unpacking and laying out our property to the best advantage. That done, we gradually began to settle down and to accommodate ourselves to our new surroundings.

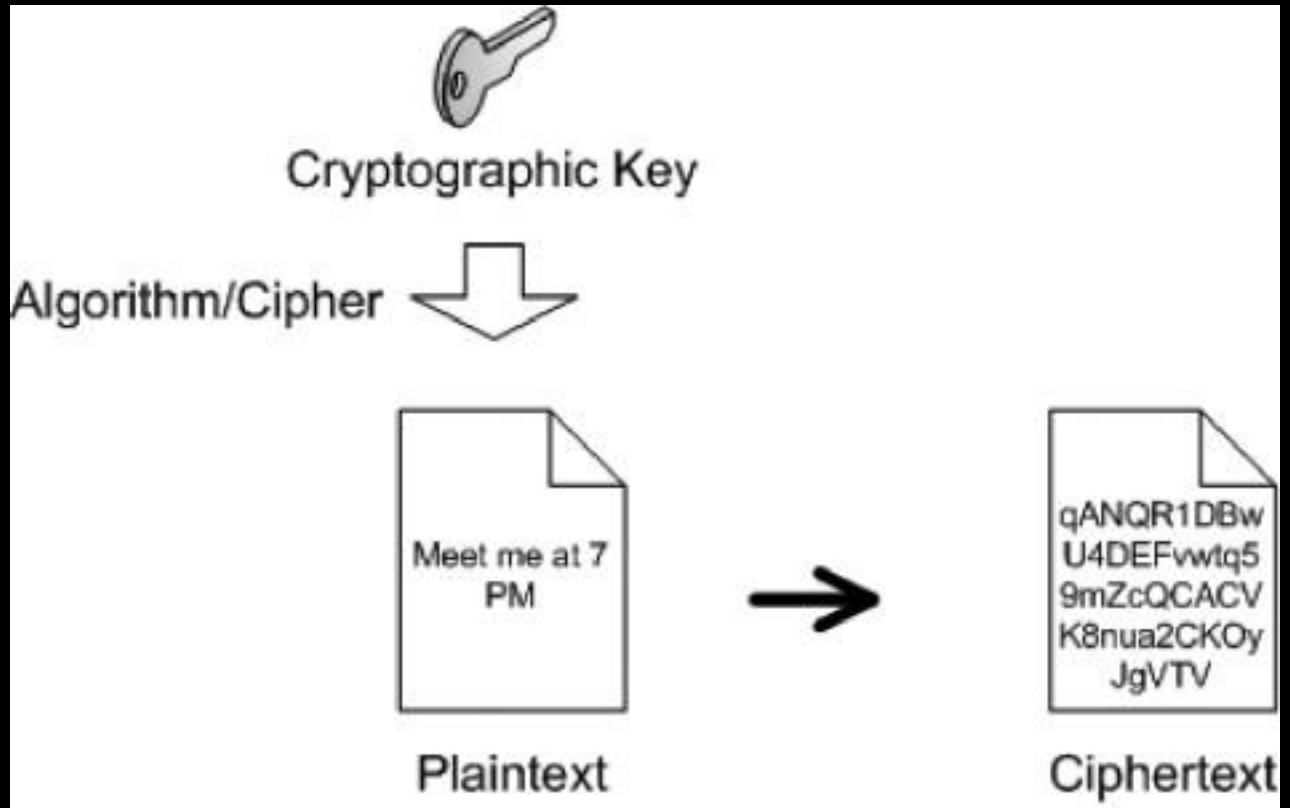
Holmes was certainly not a difficult man to live with. He was quiet in his ways, and his habits were regular. It was rare for him to be up after ten at night, and he had invariably breakfasted and gone out before I rose in the morning. Sometimes he spent his day at the chemical laboratory, sometimes in the dissecting-rooms, and occasionally in long walks, which appeared to take him into the lowest portions of the City. Nothing could exceed his energy when the working fit was upon him; but now and again a reaction would seize him, and for days on end he would lie upon the sofa in the sitting-room, hardly uttering a word or moving a muscle from morning to night. On these occasions I have noticed such a dreamy, vacant expression in his eyes, that I might have suspected him of being addicted to the use of some narcotic, had not the temperance and cleanliness of his whole life forbidden such a notion.

Ciphertext

```
From: xxxxx
To: xxxxxxxxx
Subject: xxxxxxxx
Date: Wed, xxxxxxxxx
MIME-Version: 1.0
Content-Type: multipart/encrypted; protocol="application/pgp-encrypted";
    boundary="==ztA151Vsyu96zq=-="

--==ztA151Vsyu96zq=-=
Content-Type: application/pgp-encrypted

Version: 1

--==ztA151Vsyu96zq=-=
Content-Type: application/octet-stream

-----BEGIN PGP MESSAGE-----

hQEMA2dL3e/nssauAQf9G6E9yAyFvabzd+aSIaQjOV0kme4VhHBdydBkn0lZb4mw
pJ0DV4qijjpT/Ftx4OUWtnnEu/hyjehc34fa0rJ6YAhSrfciQAvUN13WkTxa60sp
8sO9FdCGQ5xAkSoWi7YWJhD8B8+t2k8/hAZbFsJ35qGbpZcpbHPBddUA4HDV1sYA
tqLVLrV/joQZJNeNIlJCKWG8Y+IRh7EEIlQNScR6XTwULgjtwPz1TVsrTZlfzaTF
WohHcx5Wn52cRt2RmadwhaT8tPWMj+LKXrU26SPTdb94O5G//lFG3/KFJB+IOYMa
RvP+NzeoIiVxW11MmAbNrJhPYPpFS4d+1m5CkO0B2NLsAWf5a1sKOY13FCEHNTH+
6QRNdYJqEyrpnTPW8REy6J+Qqcx5WdOLKuzv0ZfZJvX20QRVHae56vHM/KoVEyZl
hgaYRcQk1jAnDOtdK7+vcWiDx+G99nW9PuXvEfFt2n/K2/RhW5xXHuR/lleec0CZ
bjergFcYgCYuqjS9p1gGf+DbP8oyRnpxrKQrd+SXuYfPM1+UZ7QZE0O/bBdeKEzW
GO1kngHGcks3UeF64KQGbm+u39br/c3nsq/yrMDY4smc1YVPLzjyHP5eq0O1e9Ay
IMddz+snYN12Nx0It/aPT3DqsDWdX2aymeGH9QPAeFUHfT7SuxPam+o70681qYWa
zTaNZsYwNjbVx446XLgu3gWPurXBK3zciddn4Jds0jaUvAqtG3kzecr8zKj8bPFr
NAebk0s0luOmkaLX1RHfi+ozGyr3u2RbCG0ubW3MDe0oIFi0bJ8yT03mK+Yzfo19
ukKSx7CXxvBQVDlQaI5iHGSi1hwodQmPDjCtBlaeTGU/g6U3wBM5WXQCbGDw/GqT
/nOEwx/7mTuRp+PzhfjyLI8s0pWWmvYVfpsuGvo0FEDLHn19uFGAMGSfWSjA2uvq
1HgIUULRVEQjBbNjxeIwN4ak1wpFHyb/aUwg908vtGEgpbf2AbUATUoewIHChi/5
M7WG5ftRkpWKZlBVtRJ7P7CNsmnBZfcgtZUvDk+YZZU4yLo7WlnFpie0gVElvauL
wWmkCuKlF3ZDiwxpBhB1aDQCWODW/aJlEUr2mHmKqpfMi2cPEI50pkRXt0rdvuyy
Lpj+uAlKSjXGQLcUVjT0dsFkSFlrwTHlkhL+h98kEdtpwN50QnbOveCFEGeQaMt+
GCWwaBSeMwC6kfZRMkmAPRoc52mq/OJ4e+HRE7cJ5p+cHx04VPDWw0m92ydQzwQw
holhBt5jheAx4zoTUrLweaVGacx/bZUo0Al4vISfYjKzNaQ2fV9hvgPuGmdaGbeF
ndsMad4+fwvOg3xuI6B2OmOJmyaMO8URgjjiZglsslVbXe2KzD/KOilpGUZ+HERu
```

Key

- The minimal secret information you hold onto



Cryptography Goals

- Without the key, ciphertext should look *random*
- Without the key, algorithm's output should be *unpredictable*
- Using the wrong key should be *detectable*
- In most cases, the action should be *binding*

Adversarial Goals

- Partially or complete recover plaintext
- Modify a message without being detected
- Impersonate someone
- Otherwise undermine the system’s guarantees

Why is randomness so important?

Why is randomness so important?

- Essential building block for *unknown information*

Pseudorandomness

- A way of amplifying true randomness

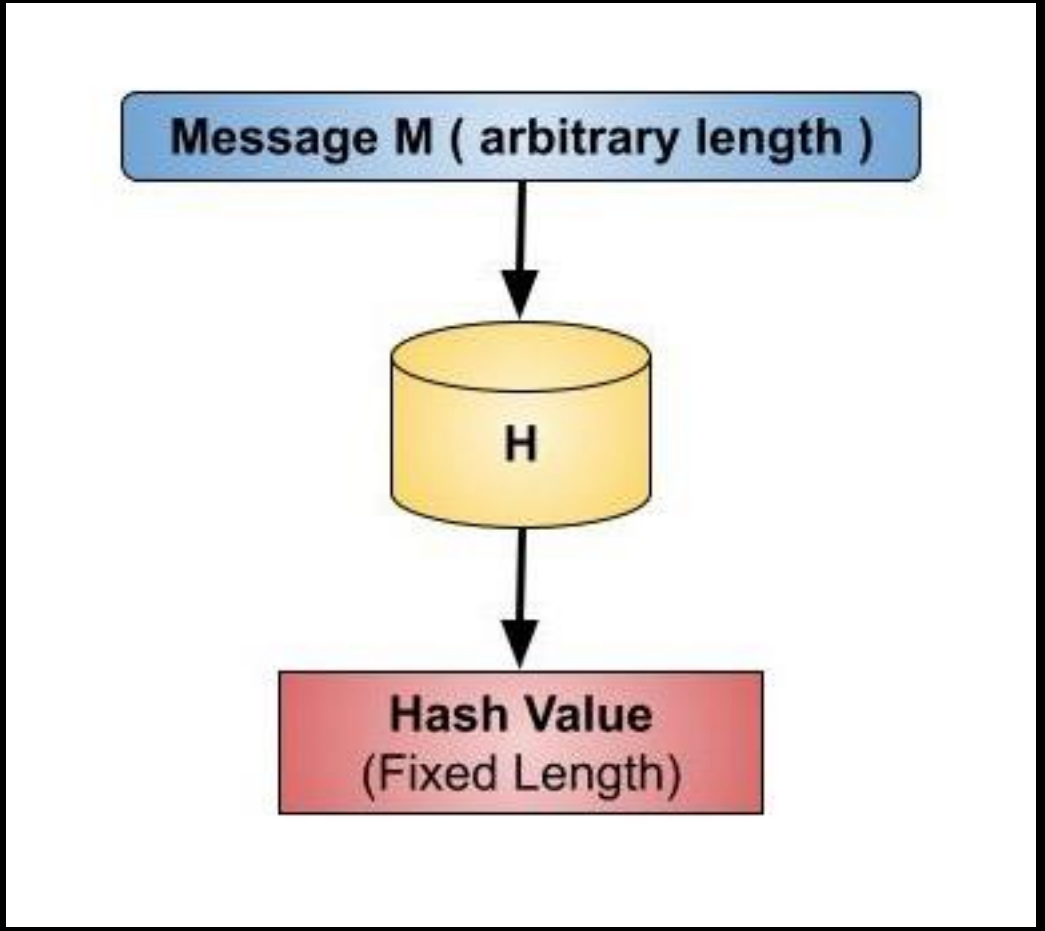
- Might actually have a pattern, but not one that a computer can figure out unless it runs for an absurdly long time

Psuedorandom Number Generator (PRNG)

- Algorithm that takes in a small (ideally random) input called a seed
  - True Random Number Generators (TRNGs) exist but are much less efficient
- Stretches this randomness to a longer stream of bits
- No computer should be able to find a pattern in the output
- Why does this provide *unpredictability*

Hash Function

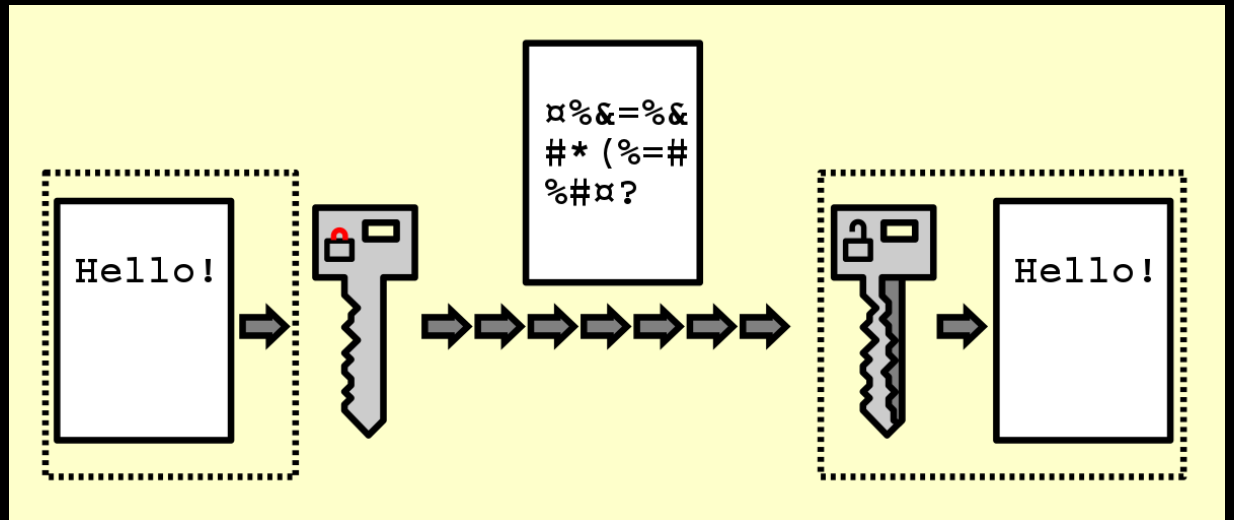
- Algorithm that takes in a message of any size, outputs a fixed size hash (also called a digest)
  - Example algo: SHA-256
- Two inputs having the same output is extremely unlikely (called a collision)
- Given only the output, hard to guess the input (One-way)
- What properties does this provide?



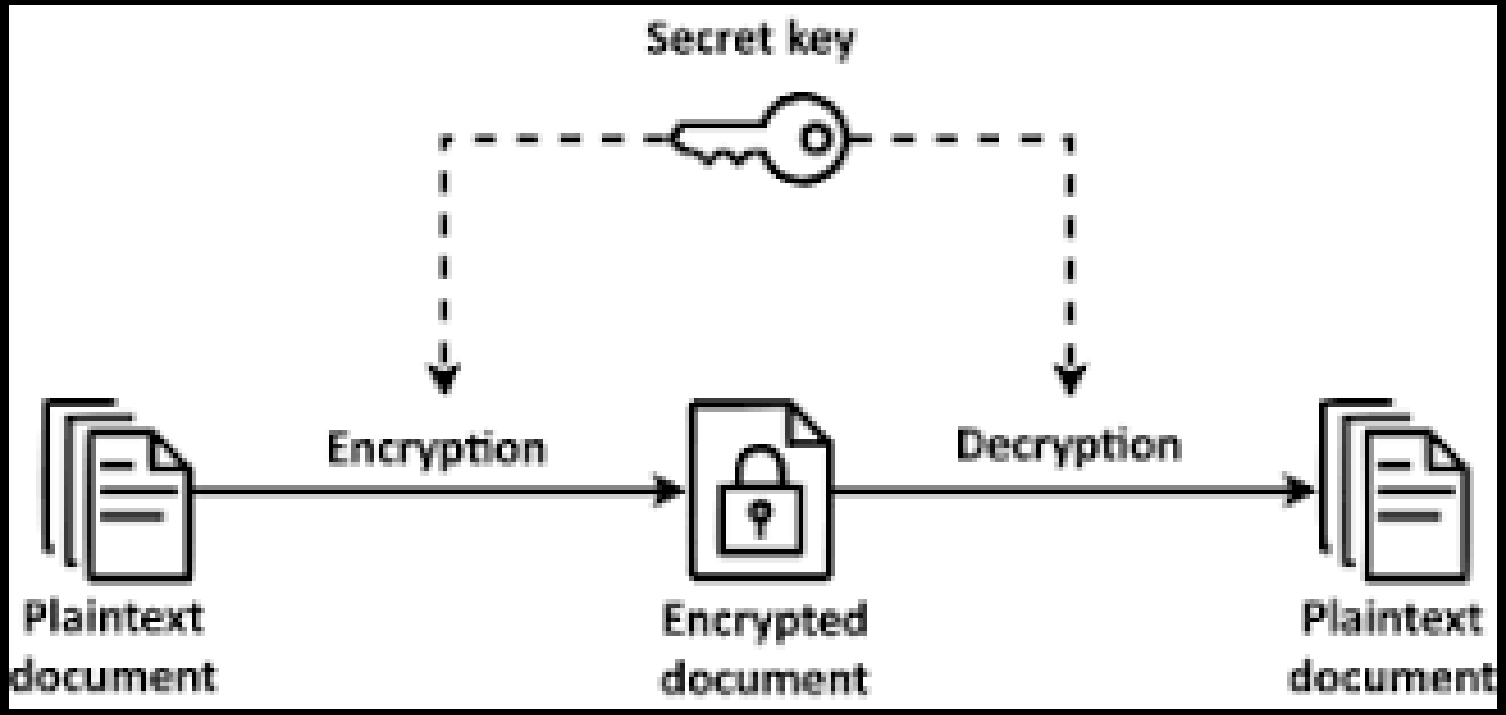
Encryption

- The operation of rendering a message indecipherable to anyone that doesn’t know the right secret information (doesn’t have the key)

- The goal is *confidentiality*



Symmetric Encryption

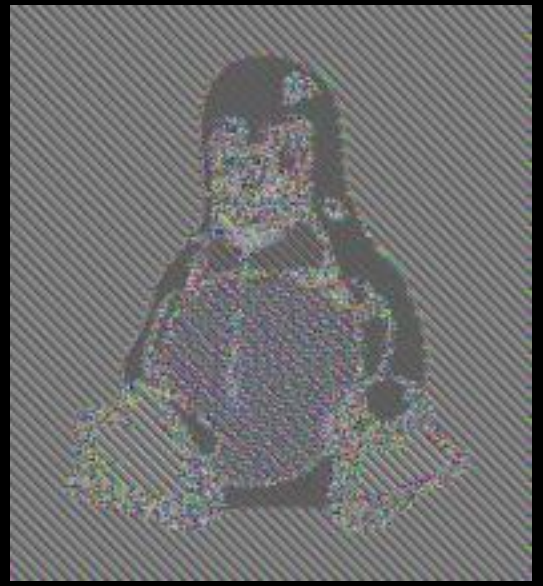


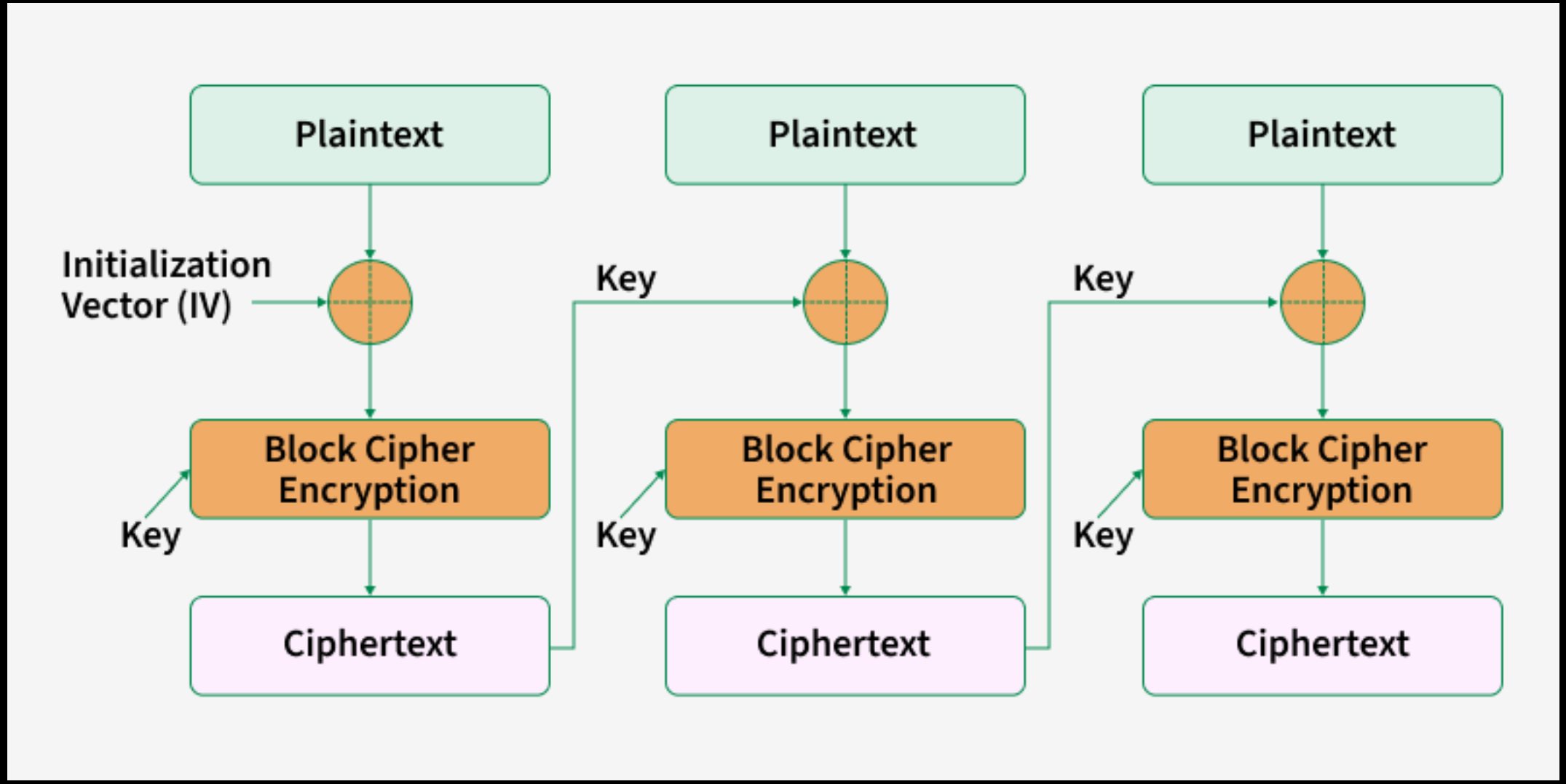
Stream Ciphers

- Encrypt messages one bit at a time
- Good for long and variable length messages
- How might we build this?
- The dream: one-time pads

Block Ciphers

- Encrypts a fixed size block of data at once
  - Example: AES
- Encrypting of multiple blocks requires special *modes of operation*
  - This is where things often go wrong
- A bit more complex in structure than stream ciphers
- Advantages?




Plaintext
Plaintext
Plaintext
Initialization Vector (IV)
Key
Key
Block Cipher Encryption
Block Cipher Encryption
Block Cipher Encryption
Key
Key
Key
Ciphertext
Ciphertext
Ciphertext

Message Authentication Codes (MACs)

- An algorithm that given a key and message produces a short *tag*
  - *EX: HMAC*

- Without the key, you cannot produce the tag (Unforgeable)

- This provides *integrity*
  - Builds on unpredictability and detectability

Authenticated Encryption

- Single algorithm that *securely* combines encryption and MAC
  - Easy to get wrong
- Most common way encryption is actually deployed
- Example: AES-GCM

How do we actually get keys?

- Different cryptographic algorithms often have their own key generation processes
- Usually some version of leveraging randomness to build a key
- Special algorithms known *as Key Derivation Functions (KDFs)* are used to generate keys
  - Passwords relate to this but more on them later

Symmetric Key downsides

Symmetric Key downsides

- Only works if both people know the key

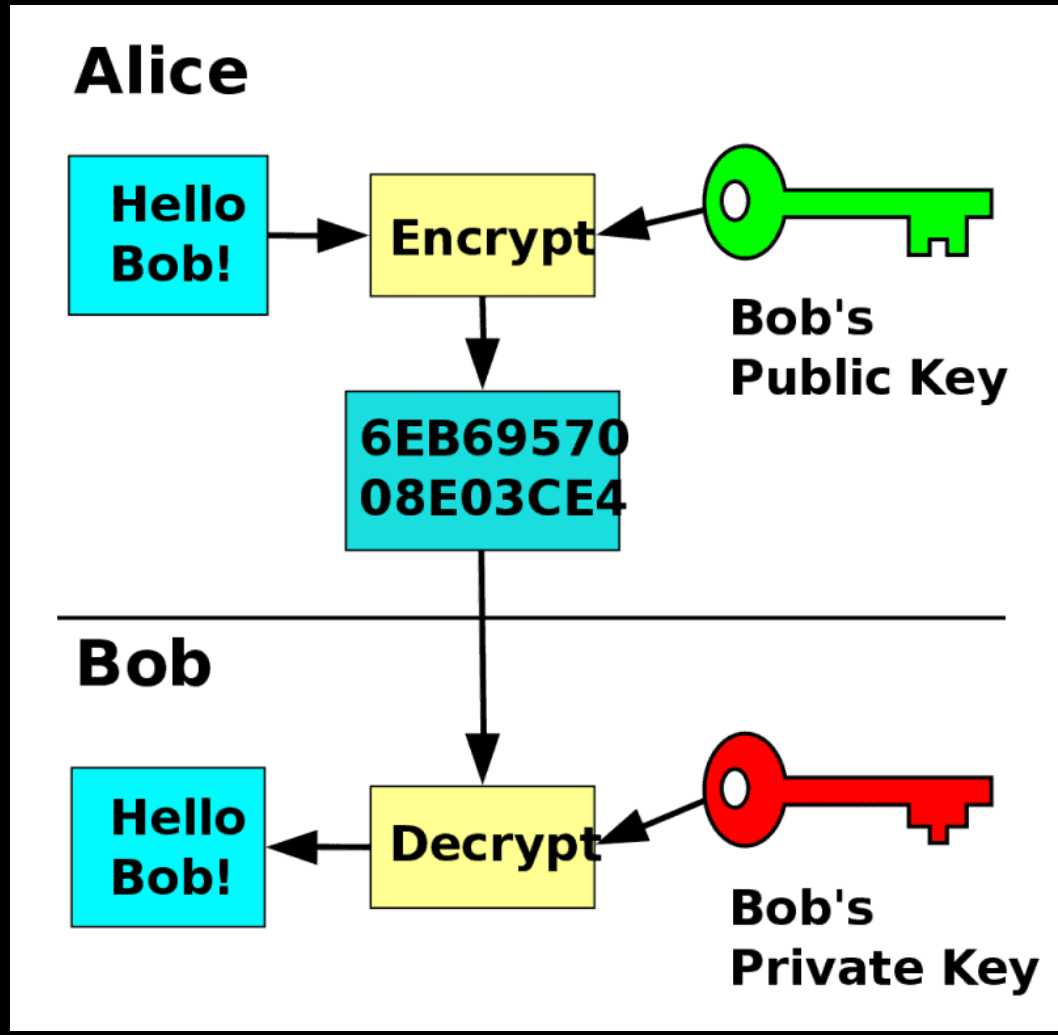
- However, we need cryptography for secure communication
  - Chicken and Egg problem

Public Key Cryptography (PKC)

- Also known as Asymmetric Key Cryptography
- Everyone has two keys
  - Public Key: Can be shared with everyone in the world, adversarial or not
  - Private Key: Don’t share with anyone
- A public key cryptosystem works as long as the matching keys are used

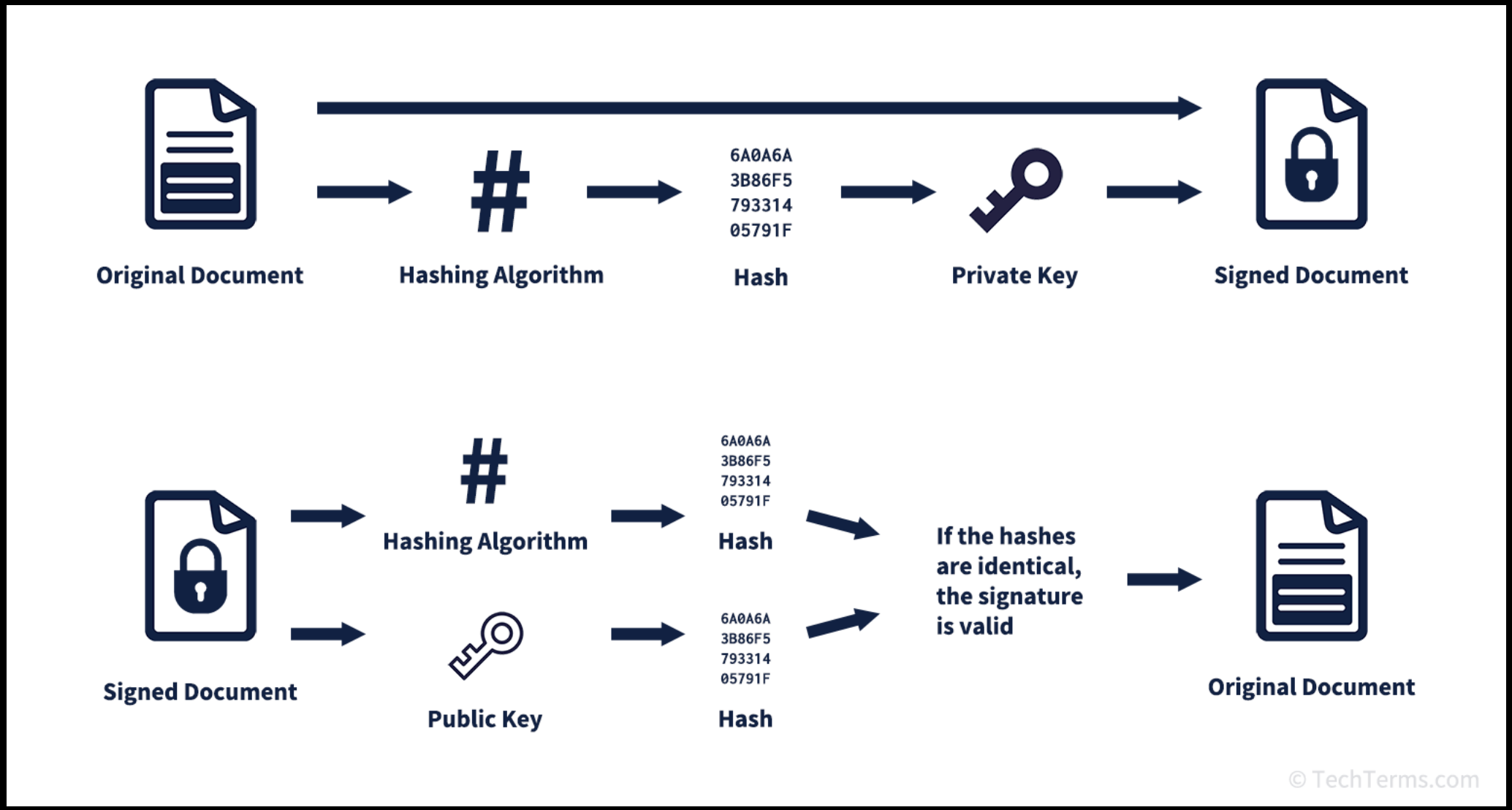
Public Key Encryption

- Everyone shares their public keys
- To encrypt a message to someone, you use their public key as input
- Need the matching private key to decrypt
  - Only the recipient knows this key
- Examples: RSA, ElGamal



Digital Signatures

- PKC can be used for more than encryption, it can also provide *authenticity* or proof of identity
- Since only you know the private key matching your public key, this can serve as a form of identification
- Digital Signatures leverage this to authenticate messages


Original Document
Hashing Algorithm
6A0A6A
3B86F5
793314
05791F
Hash
Private Key
Signed Document
Signed Document
Hashing Algorithm
6A0A6A
3B86F5
793314
05791F
Hash
Public Key
6A0A6A
3B86F5
793314
05791F
Hash
If the hashes are identical, the signature is valid
Original Document
© TechTerms.com

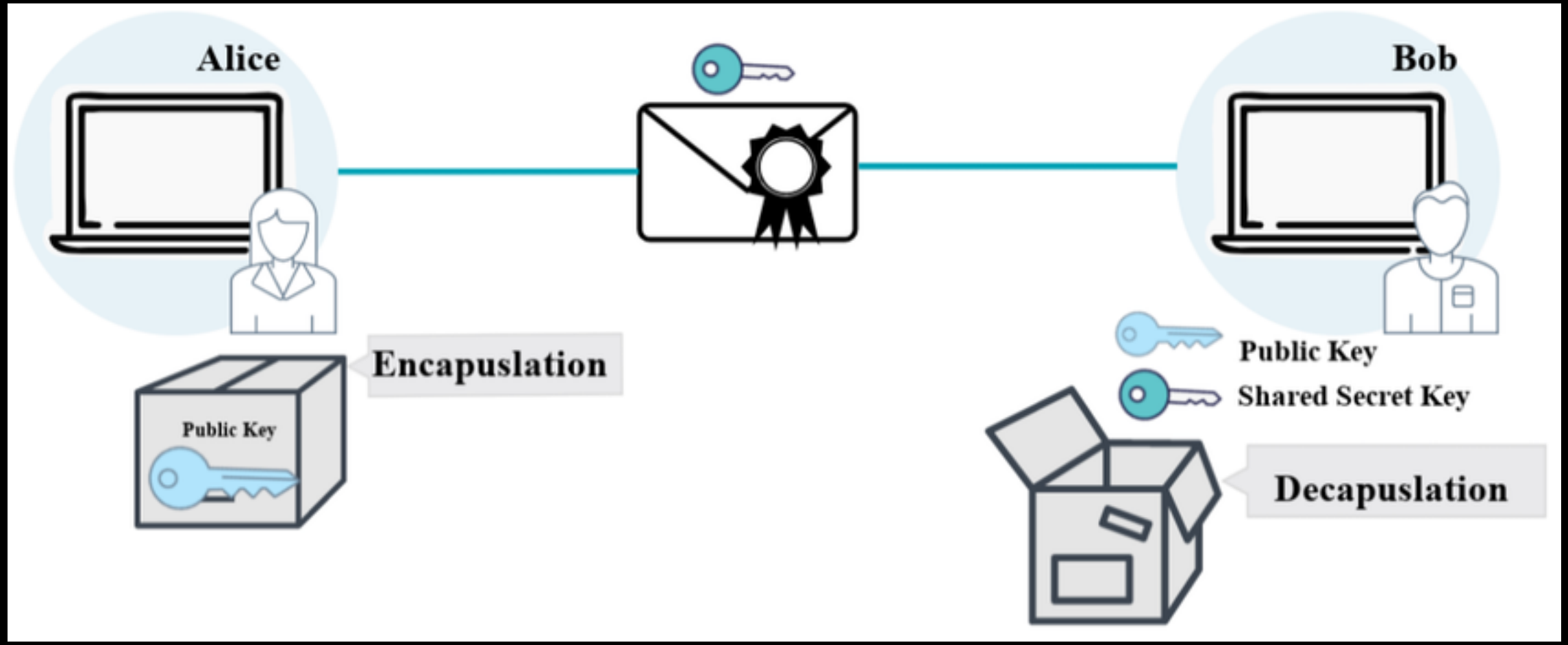
Public Key downsides

- Public Key algorithms are significantly slower than symmetric key operations
- Also still need some trusted infrastructure to support
  - But we will focus on that later
- What can we do?

Hybrid Encryption

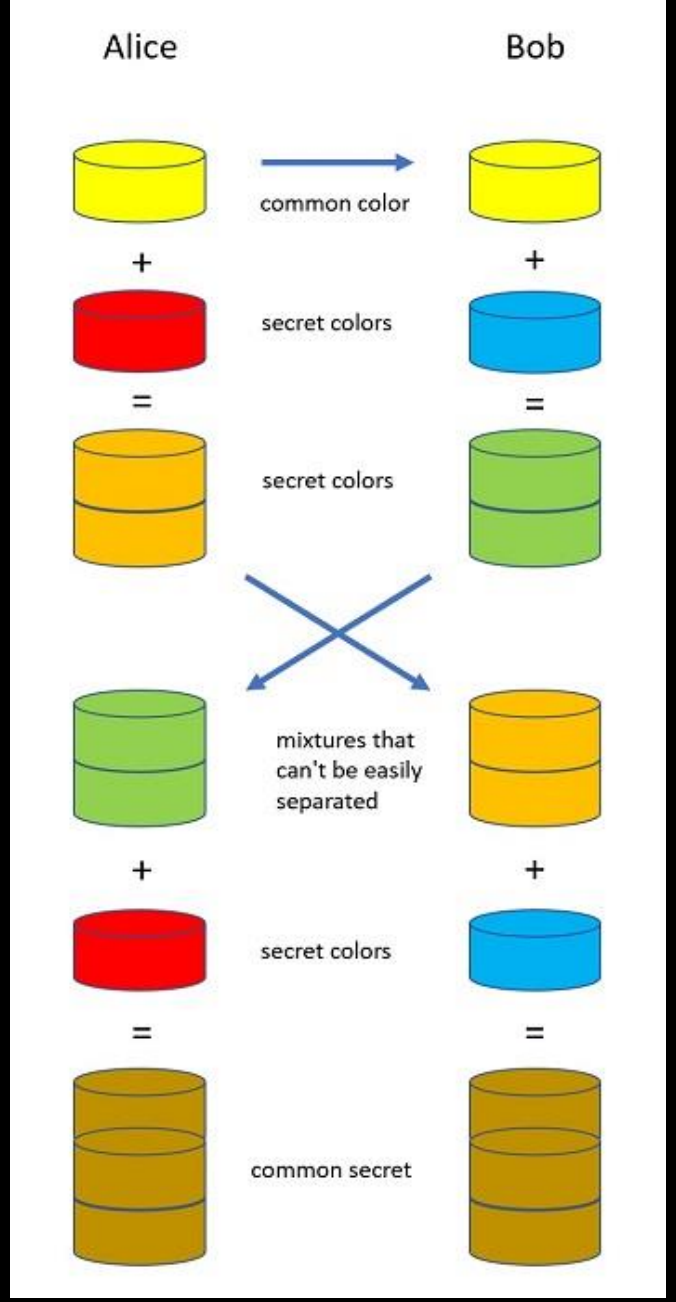
- The best of both worlds
- Use PKC to securely share symmetric keys
- Use the symmetric keys for everything else

Key Encapsulation Mechanisms



Key Exchange/Key Agreement

- Interactive proceed to arrive at a shared key to be used
- Should not reveal anything secret in the clear
- Analogy: Locked Box



https://jamesmccaffrey.wordpress.com/2020/07/29/the-diffie-hellman-key-exchange/

Next Time

- Differential Privacy
- Other Mechanisms for Privacy