CODATA – RDA

Data Schools

Information Security

Raphael Cobe raphaelmcobe@gmail.com

~~Why Security?~~

~~Data Security Concepts~~

~~Security Objectives~~

~~Guidelines and Principles~~

Introduction to Encryption

Hash Functions

Certificates

Thanks

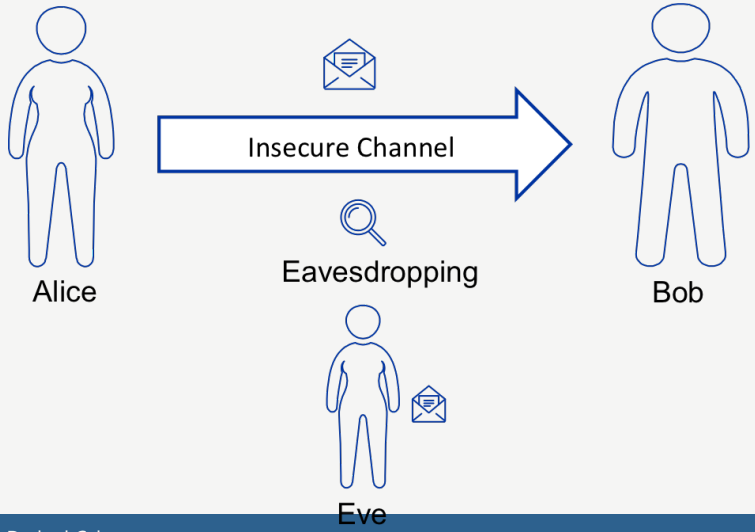
- These slide are a (small) variation of the presentation by Hannah Short

Data Schools

Section 5

Introduction to Encryption

Why Encryption?



Why Encryption?

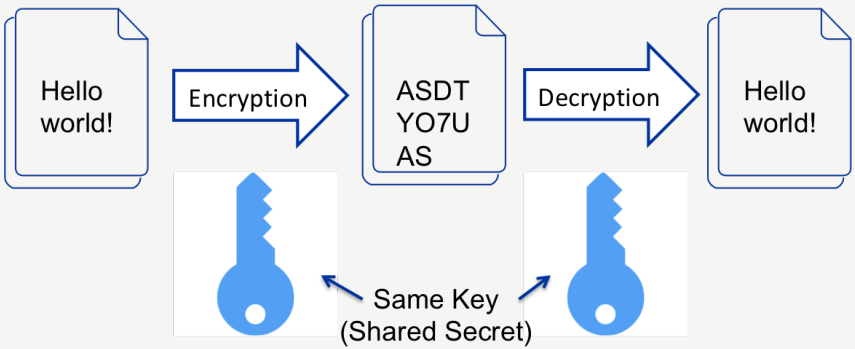
What are the goals?

- **Confidentiality**: To prevent adversaries from viewing/accessing messages
- **Integrity**: To prevent adversaries from silently modifying messages
- **Authentication**: To prevent adversaries from impersonating an identity
- **Non-repudiation**: To prevent adversaries from denying an action

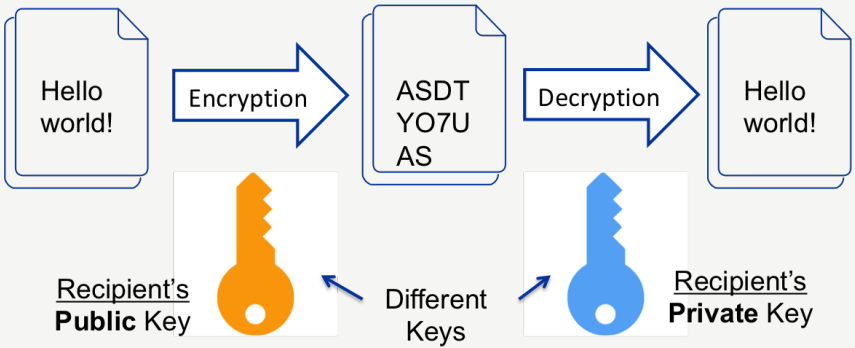
Encryption in practice

- There are several common, robust encryption algorithms available (e.g. AES and RSA)
- A good encryption algorithm relies on keeping the key secret, not the cipher algorithm itself!
- Choose a well known, secure algorithm and keep the key secure (do not trust proprietary algorithms)
- There are two main types; **Symmetric and Asymmetric**

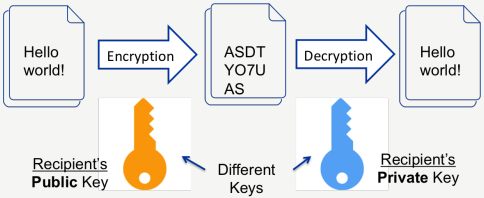
Symmetric Encryption



Asymmetric Encryption



Asymmetric Encryption



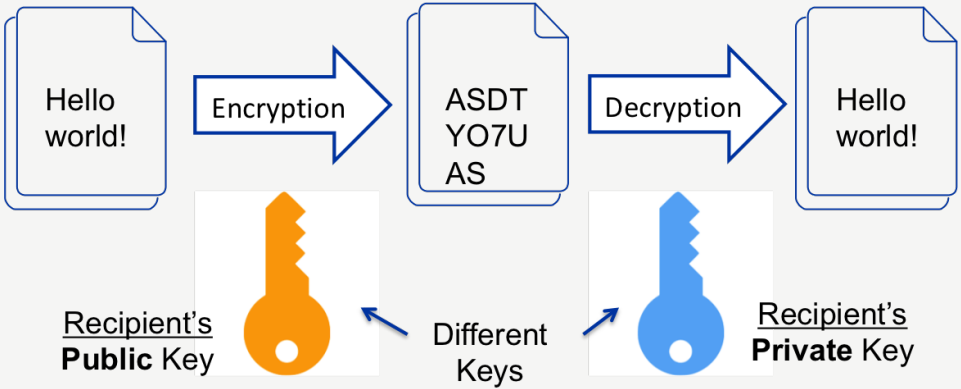
2 interchangeable (linked) keys

- Public + Private
- Mathematically difficult to compute one from the other
- 1 for encryption and the other decryption

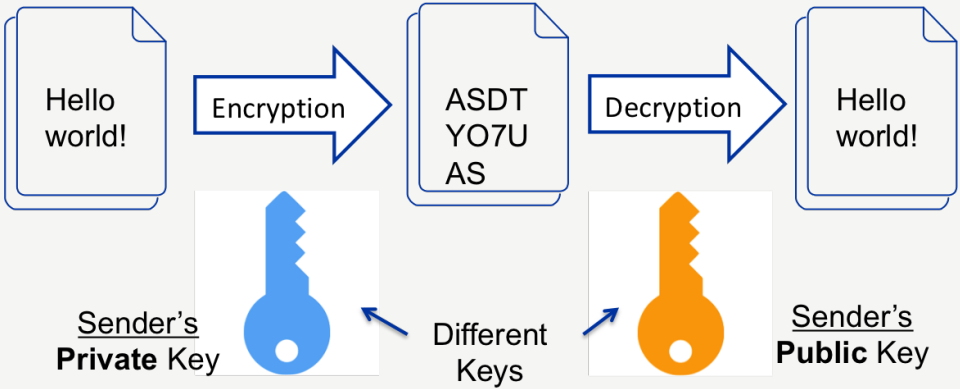
Asymmetric Encryption

- Relies on the fact that it is **easy** to multiply primes but hard to factorise their product
- Consider the number 221... what are its factors?
- Security is dependent on the status of computing technologies (it's secure now, but won't be in 100 years...)

Asymmetric Enc. - Confidentiality



Asymmetric Enc. - Authentication



Encryption - Summary

- Encryption can be used for confidential, authenticated communication
- Symmetric and Asymmetric Ciphers have evolved over time

Data Schools

Section 6

Hash Functions

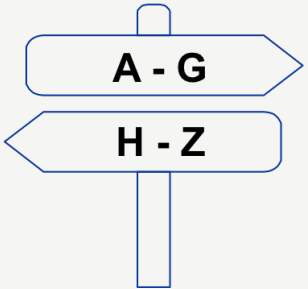
Hash Functions

A hash function is any function that can be used to map data of arbitrary size to data of a fixed size.

Hash Functions

How can we make something of a fixed length?

- We want the input (however long) to turn into one of a smaller range of possible outputs
- Consider a registration process where attendees pick up their badges based on the first letter of surname...



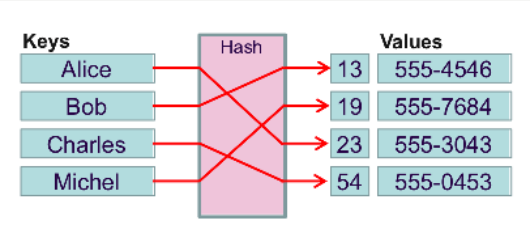
Hash Functions

E.g. *"Today is gonna be the day that they're gonna throw it back to you. By now you should've somehow realized what you gotta do. I don't believe that anybody feels the way I do, about you now"* becomes **0283bf5eb0c60213a99f011a89300179** using the MD5 hashing algorithm
`https://passwordsgenerator.net/md5-hash-generator/`

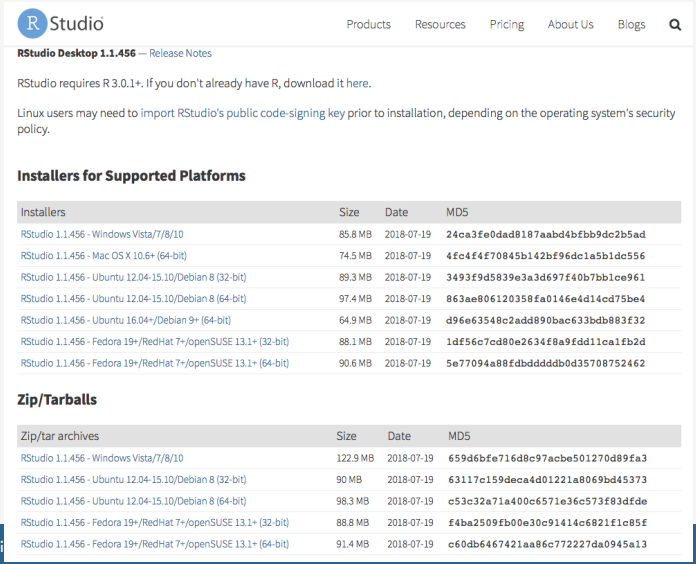
Hash Functions

What is a *good* hash function? For $h = hash(m)$

- Difficult to find any message m with a given hash value h
- Difficult to find 2 messages $m1$, $m2$ such that: $hash(m1) = hash(m2)$



Hash Functions - a Use Case



RStudio Products Resources Pricing About Us Blogs

RStudio Desktop 1.1.456 — Release Notes

RStudio requires R 3.0.1+. If you don't already have R, download it here.

Linux users may need to import RStudio's public code-signing key prior to installation, depending on the operating system's security policy.

Installers for Supported Platforms

Installers	Size	Date	MD5
RStudio 1.1.456 - Windows Vista/7/8/10	85.8 MB	2018-07-19	24ca3fe0dad8187aabd4bfbb9dc2b5ad
RStudio 1.1.456 - Mac OS X 10.6+ (64-bit)	74.5 MB	2018-07-19	4fc4f4f70845b142bf96dc1a5b1dc556
RStudio 1.1.456 - Ubuntu 12.04-15.10/Debian 8 (32-bit)	89.3 MB	2018-07-19	3493f9d5839e3a3d697f40b7bb1ce961
RStudio 1.1.456 - Ubuntu 12.04-15.10/Debian 8 (64-bit)	97.4 MB	2018-07-19	863ae806120358fa0146e4d14cd75be4
RStudio 1.1.456 - Ubuntu 16.04+/Debian 9+ (64-bit)	64.9 MB	2018-07-19	d96e63548c2add890bac633bdb883f32
RStudio 1.1.456 - Fedora 19+/RedHat 7+/openSUSE 13.1+ (32-bit)	88.1 MB	2018-07-19	1df56c7cd80e2634f8a9fdd11ca1fb2d
RStudio 1.1.456 - Fedora 19+/RedHat 7+/openSUSE 13.1+ (64-bit)	90.6 MB	2018-07-19	5e77094a88fdbdddddb0d35708752462

Zip/Tarballs

Zip/tar archives	Size	Date	MD5
RStudio 1.1.456 - Windows Vista/7/8/10	122.9 MB	2018-07-19	659d6bfe716d8c97acbe501270d89fa3
RStudio 1.1.456 - Ubuntu 12.04-15.10/Debian 8 (32-bit)	90 MB	2018-07-19	63117c159deca4d01221a8069bd45373
RStudio 1.1.456 - Ubuntu 12.04-15.10/Debian 8 (64-bit)	98.3 MB	2018-07-19	c53c32a71a400c6571e36c573f83dfde
RStudio 1.1.456 - Fedora 19+/RedHat 7+/openSUSE 13.1+ (32-bit)	88.8 MB	2018-07-19	f4ba2509fb00e30c91414c6821f1c85f
RStudio 1.1.456 - Fedora 19+/RedHat 7+/openSUSE 13.1+ (64-bit)	91.4 MB	2018-07-19	c60db6467421aa86c772227da0945a13

Hash Functions - another Use Case

- Instead of storing passwords, secure services store their hashes!
- What would happen if the database is compromised?

Hash Functions - another Use Case

- Instead of storing passwords, secure services store their hashes!
- What would happen if the database is compromised?
  - **Dictionary attacks still valid**
  - This can be avoided by "salting" passwords, the system adds digits before hashing

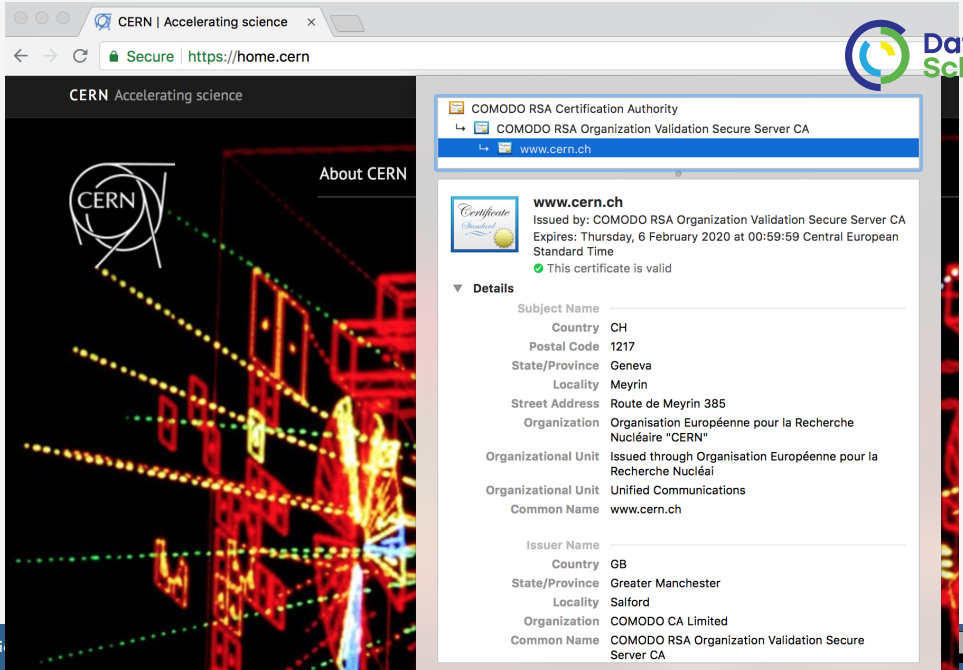
Hash Functions - Summary

- Hash functions transform arbitrary data to a fixed size in a deterministic (repeatable) way
- There are multiple applications, e.g. file integrity & password storage

Data Schools

Section 7

Certificates


CERN | Accelerating science
Secure
https://home.cern
CERN Accelerating science
About CERN
COMODO RSA Certification Authority
COMODO RSA Organization Validation Secure Server CA
www.cern.ch
www.cern.ch
Issued by: COMODO RSA Organization Validation Secure Server CA
Expires: Thursday, 6 February 2020 at 00:59:59 Central European Standard Time
This certificate is valid
Details
Subject Name
Country CH
Postal Code 1217
State/Province Geneva
Locality Meyrin
Street Address Route de Meyrin 385
Organization Organisation Européenne pour la Recherche Nucléaire "CERN"
Organizational Unit Issued through Organisation Européenne pour la Recherche Nucléai
Organizational Unit Unified Communications
Common Name www.cern.ch
Issuer Name
Country GB
State/Province Greater Manchester
Locality Salford
Organization COMODO CA Limited
Common Name COMODO RSA Organization Validation Secure Server CA

Certificates

What is a certificate? A digital document that:

- Contains identity information
- Contains a public key (this is public information)
- Is digitally “signed" by a trusted body

Certificates are accompanied by private keys (kept secret by the owner!)

Certificate Authentication

Owning a Certificate of Alice does not mean that you are Alice

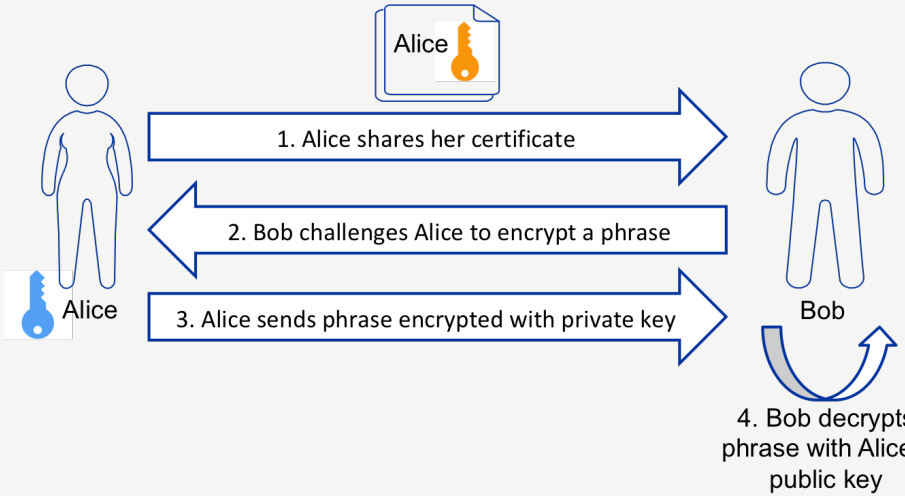
- Holding a Certificate does not imply you are authenticated
- How would you verify that the person who comes to you pretending to be Alice and showing you a certificate of Alice is really Alice ?

Certificate Authentication

Owning a Certificate of Alice does not mean that you are Alice

- Holding a Certificate does not imply you are authenticated
- How would you verify that the person who comes to you pretending to be Alice and showing you a certificate of Alice is really Alice ?
  - **You have to challenge her!**
  - Only the real Alice has the private key that goes in pair with the public key in the certificate.

Certificate Authentication



Certificates - Summary

- Contain a public key and identity information
- Certificates are validated by Certificate Authorities
- Certificates & private keys together allow asymmetric encryption and authentication

Questions?

- Ask now
- Find us during the break
- You are welcome to contact us after the school