Cryptography - Anonymity - SFSU CyberSec Team

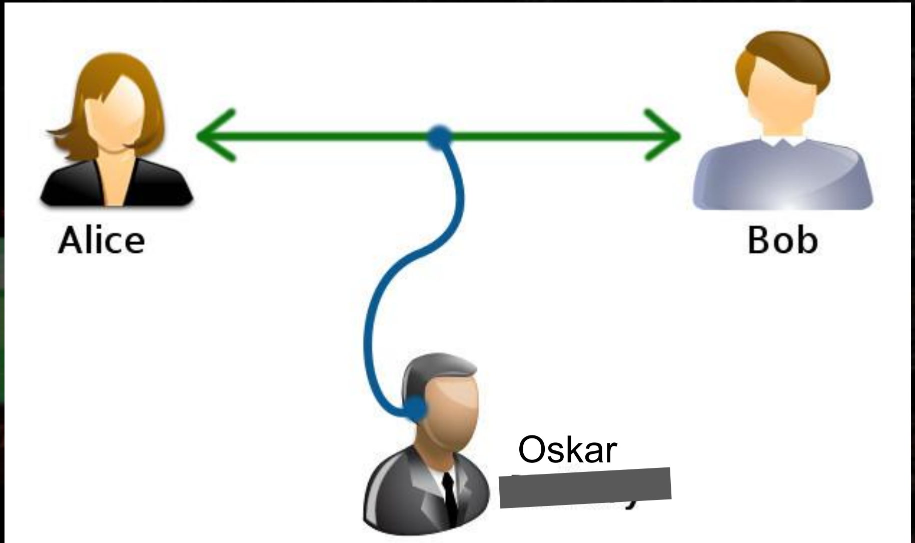
Discord

Current Agenda for today.

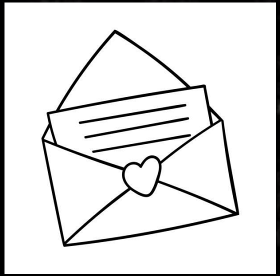
- Basics of cryptography
- Modern forms of cryptography
- Introduction to anonymity online
- Further resources / material

What is cryptography? What does it aim to solve?

Let’s describe a scenario with Alice, Bob, and Oskar

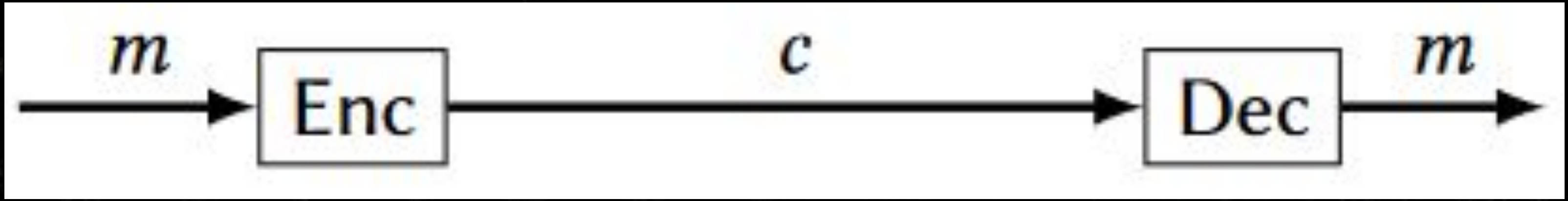


Alice wants to send a message to Bob, but any message sent will be intercepted and possibly read by Oskar!!



Let Alice and Bob share some secret before initiating the conversion. Maybe that can prevent eavesdropping?

The idea is to make the message meaningless to oskar, but valuable to our recipients.

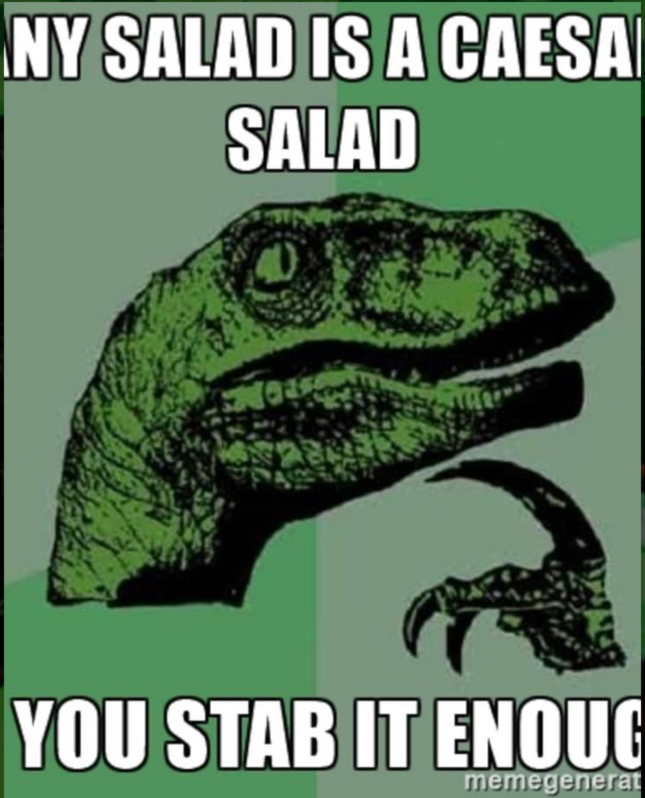


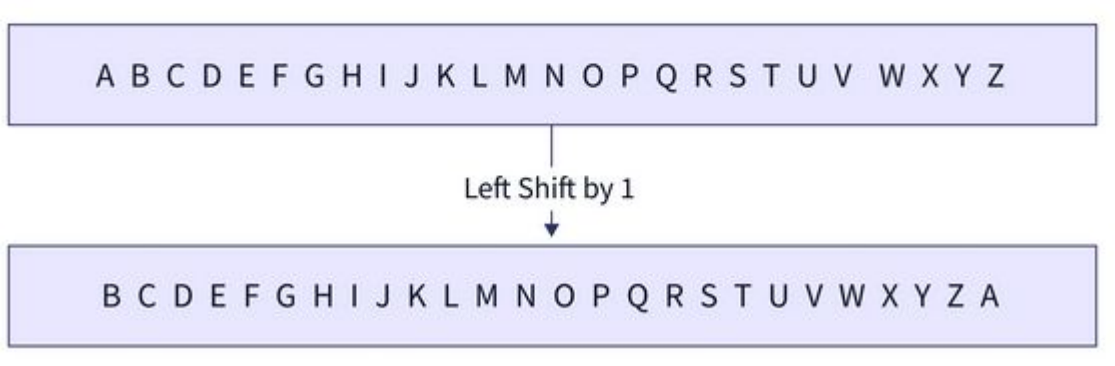
Plaintext - The decrypted message
Ciphertext - The encrypted message
Secret key - 🤫🤫🤫🤫🤫🤫🤫🤫🤫🤫🤫🤫🤫

The great problems of cryptography.

- Weak encryption - can be deciphered easily.
- Key distribution - how will you share the secret?
- Availability - how will we know if the message will be received by the other end?
- Randomness is evil.
- Authentication - how will we know if the message has been tampered with?

Earliest recognized examples of cryptography




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

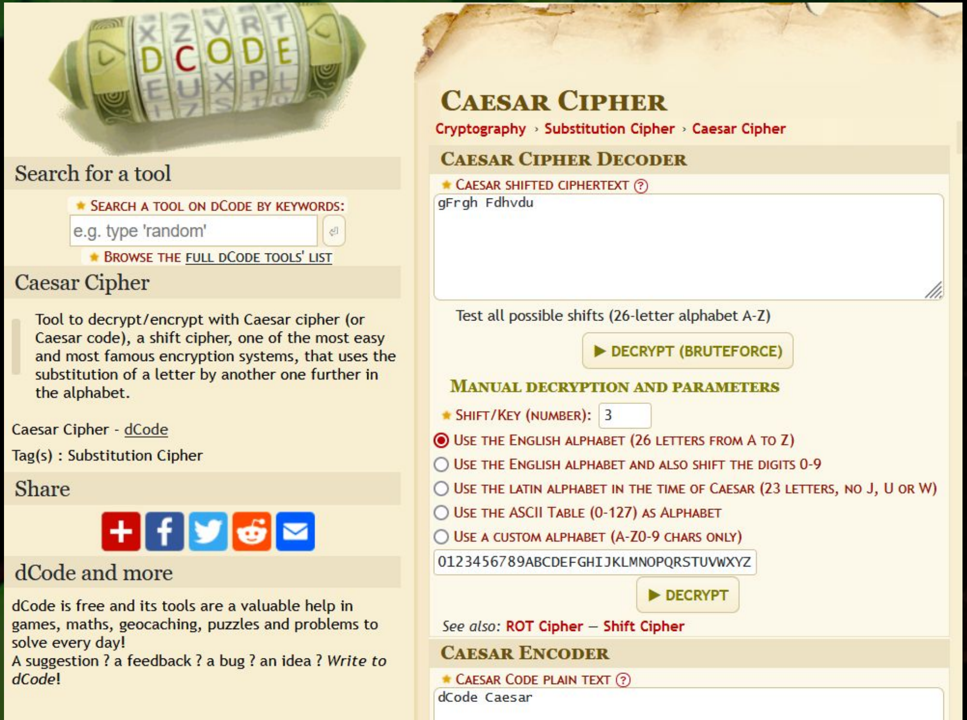
Left Shift by 1

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

Very weak key space - 26 keys

Very easy to brute force.

https://www.dcode.fr/caesar-cipher


Search for a tool
★ Search a tool on dCode by keywords:
e.g. type 'random'
★ Browse the full dCode tools' list

Caesar Cipher

Tool to decrypt/encrypt with Caesar cipher (or Caesar code), a shift cipher, one of the most easy and most famous encryption systems, that uses the substitution of a letter by another one further in the alphabet.

Caesar Cipher - dCode

Tag(s) : Substitution Cipher

dCode and more

dCode is free and its tools are a valuable help in games, maths, geocaching, puzzles and problems to solve every day!
A suggestion ? a feedback ? a bug ? an idea ? *Write to dCode*!

Caesar Cipher

Caesar Cipher Decoder

★ Caesar shifted ciphertext ?

```
gFrgh Fdhvdu
```

Test all possible shifts (26-letter alphabet A-Z)

Manual decryption and parameters

★ Shift/Key (number): 3

● Use the English alphabet (26 letters from A to Z)
○ Use the English alphabet and also shift the digits 0-9
○ Use the Latin alphabet in the time of Caesar (23 letters, no J, U or W)
○ Use the ASCII table (0-127) as alphabet
○ Use a custom alphabet (A-Z0-9 chars only)

0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ

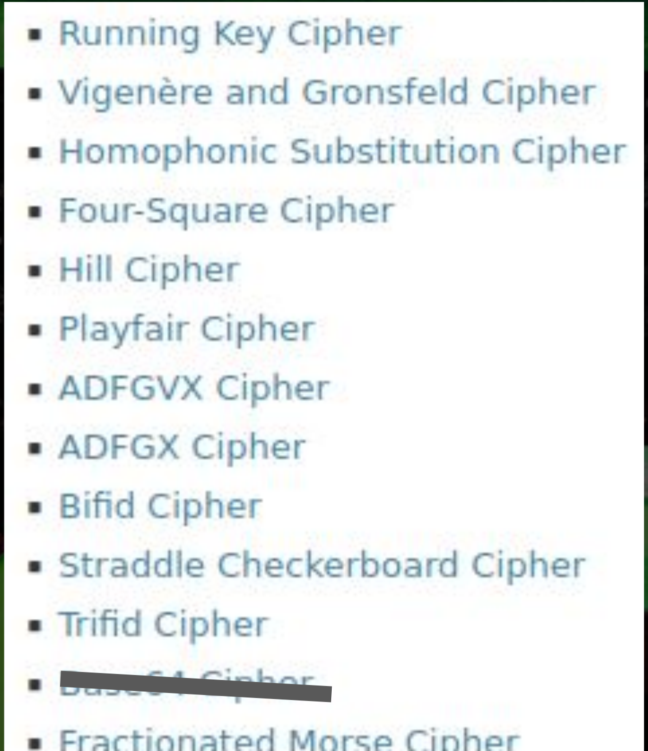
See also: ROT Cipher – Shift Cipher

Caesar Encoder

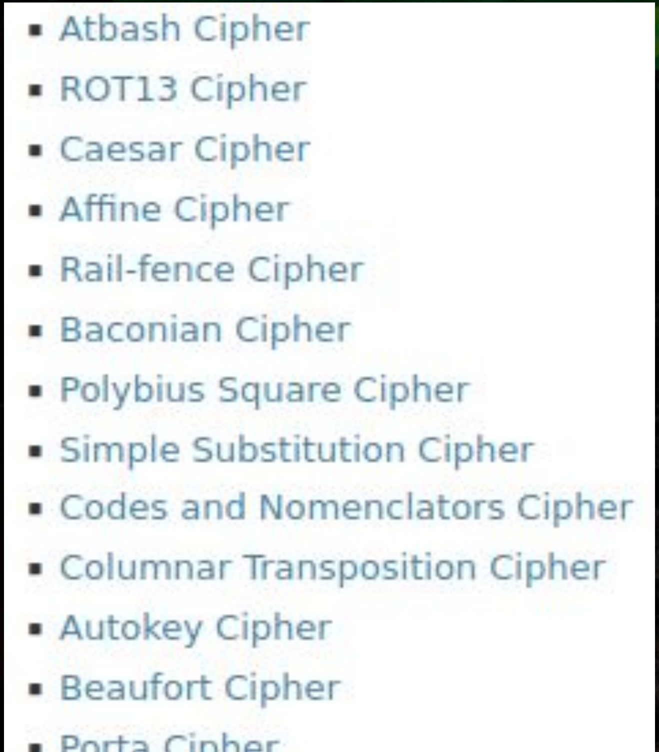
★ Caesar code plain text ?

```
dCode Caesar
```

Civilization advances, and more complicated ciphers emerge. Secrets are exchanged and algorithms are shared. Here are some “ciphers” that were invented pre-computer era.

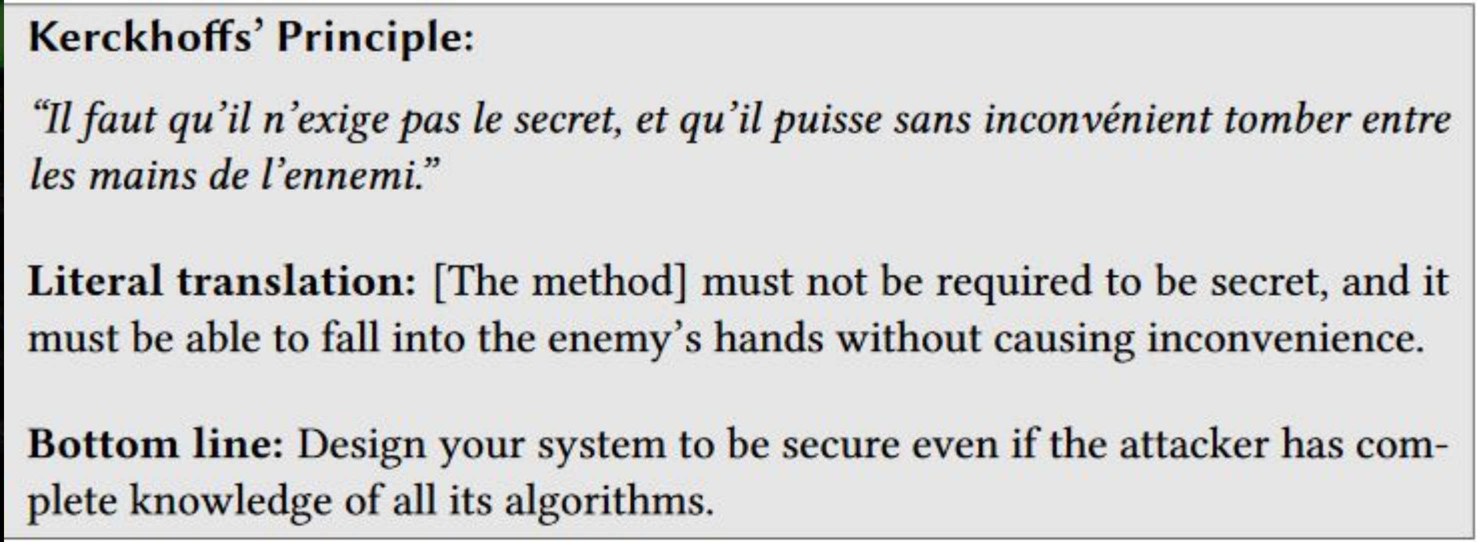


- Running Key Cipher
- Vigenère and Gronsfeld Cipher
- Homophonic Substitution Cipher
- Four-Square Cipher
- Hill Cipher
- Playfair Cipher
- ADFGVX Cipher
- ADFGX Cipher
- Bifid Cipher
- Straddle Checkerboard Cipher
- Trifid Cipher
- ~~Base64 Cipher~~
- Fractionated Morse Cipher



- Atbash Cipher
- ROT13 Cipher
- Caesar Cipher
- Affine Cipher
- Rail-fence Cipher
- Baconian Cipher
- Polybius Square Cipher
- Simple Substitution Cipher
- Codes and Nomenclators Cipher
- Columnar Transposition Cipher
- Autokey Cipher
- Beaufort Cipher
- Porta Cipher

Two principles that share any relevance to modern cryptography



Kerckhoffs' Principle:

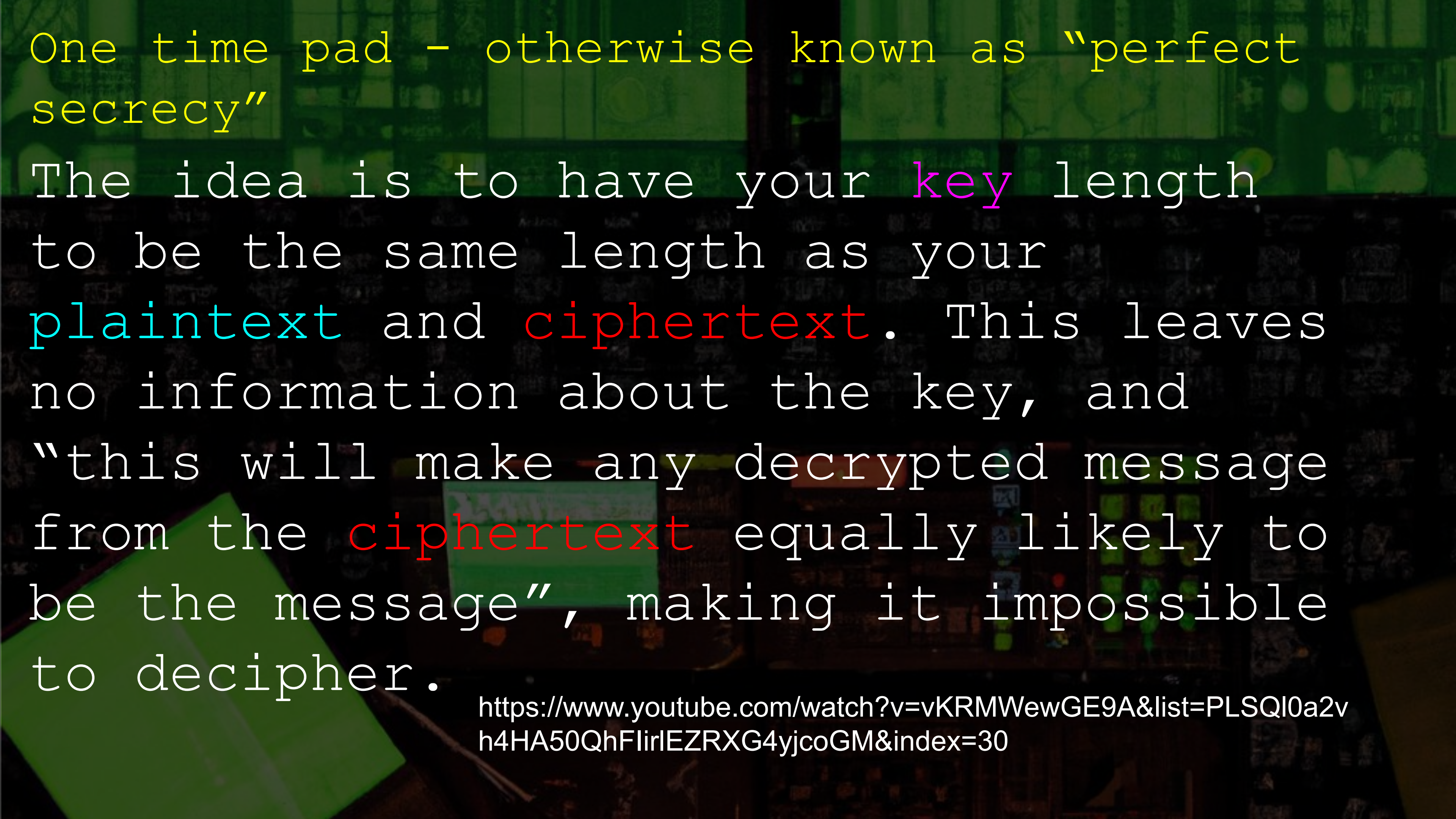
"Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi."

Literal translation: [The method] must not be required to be secret, and it must be able to fall into the enemy's hands without causing inconvenience.

Bottom line: Design your system to be secure even if the attacker has complete knowledge of all its algorithms.

1)

2) **One time pad**



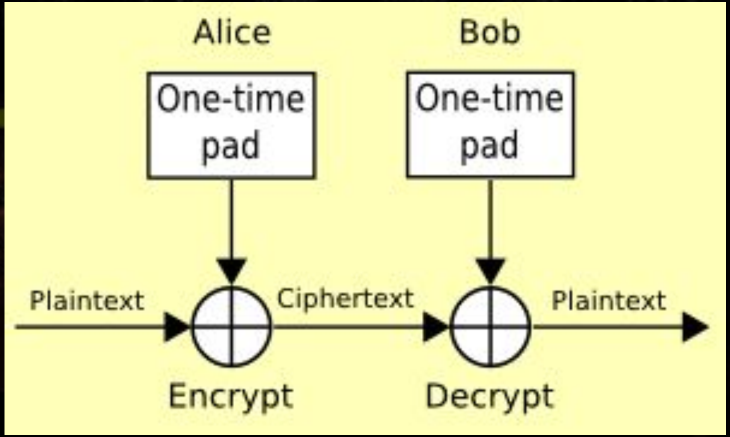
One time pad - otherwise known as “perfect secrecy”

The idea is to have your key length to be the same length as your plaintext and ciphertext. This leaves no information about the key, and “this will make any decrypted message from the ciphertext equally likely to be the message”, making it impossible to decipher.

https://www.youtube.com/watch?v=vKRMWewGE9A&list=PLSQl0a2vh4HA50QhFIirlEZRXG4yjcoGM&index=30

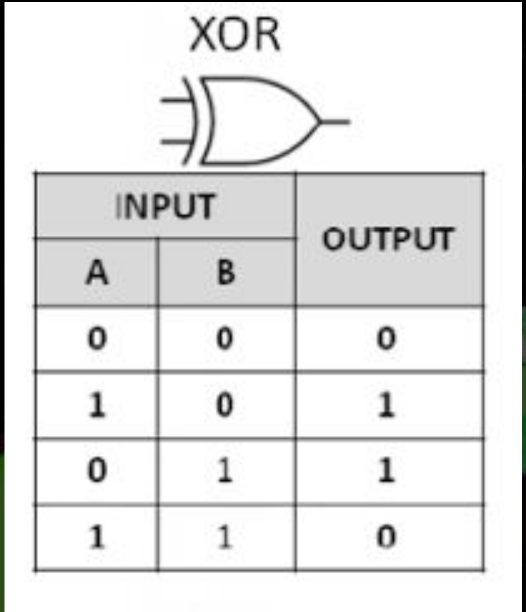
Caveats to OTP (One-Time-Pad)

- ❑ You can only use the key once (failing to do so leaks information about the key!)
- ❑ Should be random - randomness is evil
- ❑ Sharing the key! - key distribution strikes again.



Break time!

What is xor?
In some ways it is an encryption scheme!



INPUT		OUTPUT
A	B	
0	0	0
1	0	1
0	1	1
1	1	0

Here’s a string

“]]_”
Now xor it with “123”
Tell me what you get

How I like to think of xor - if A and B are different, return true, otherwise return false.

Principles of Modern Cryptography

Symmetric encryption - uses the same key for both encryption and decryption.

Examples include - **DES, AES**

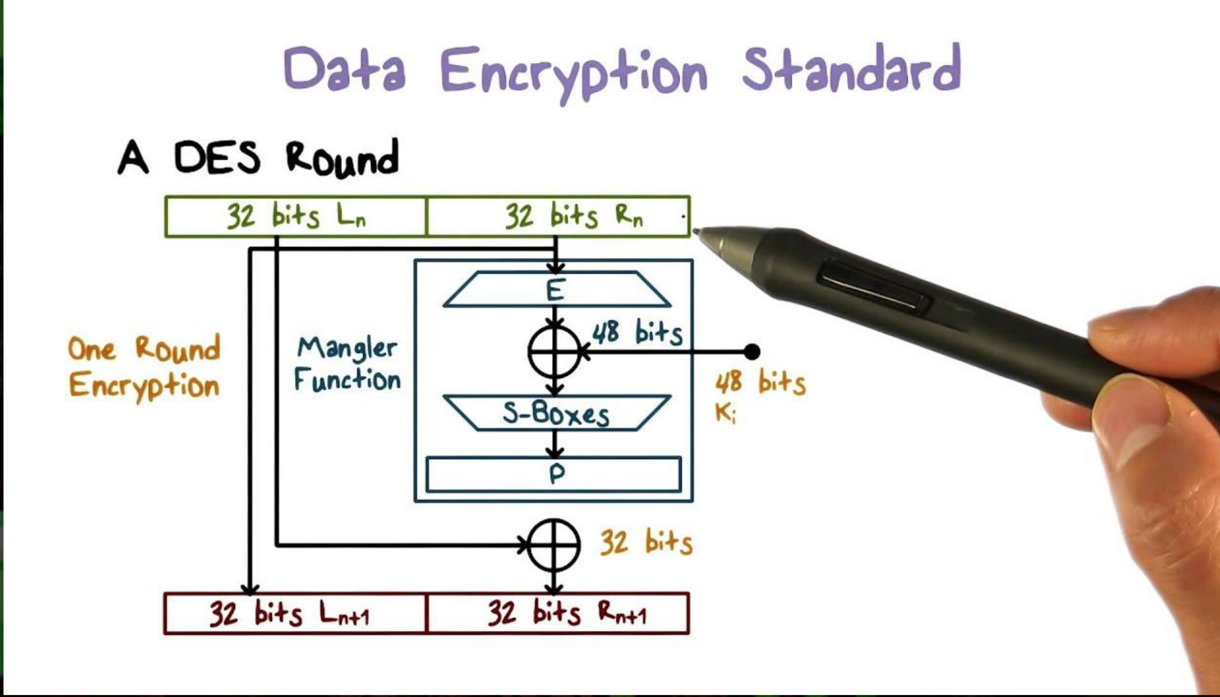
Asymmetric encryption - uses two separate keys to encrypt and decrypt.

Popular examples include - **Diffie-Hellman exchange, RSA**

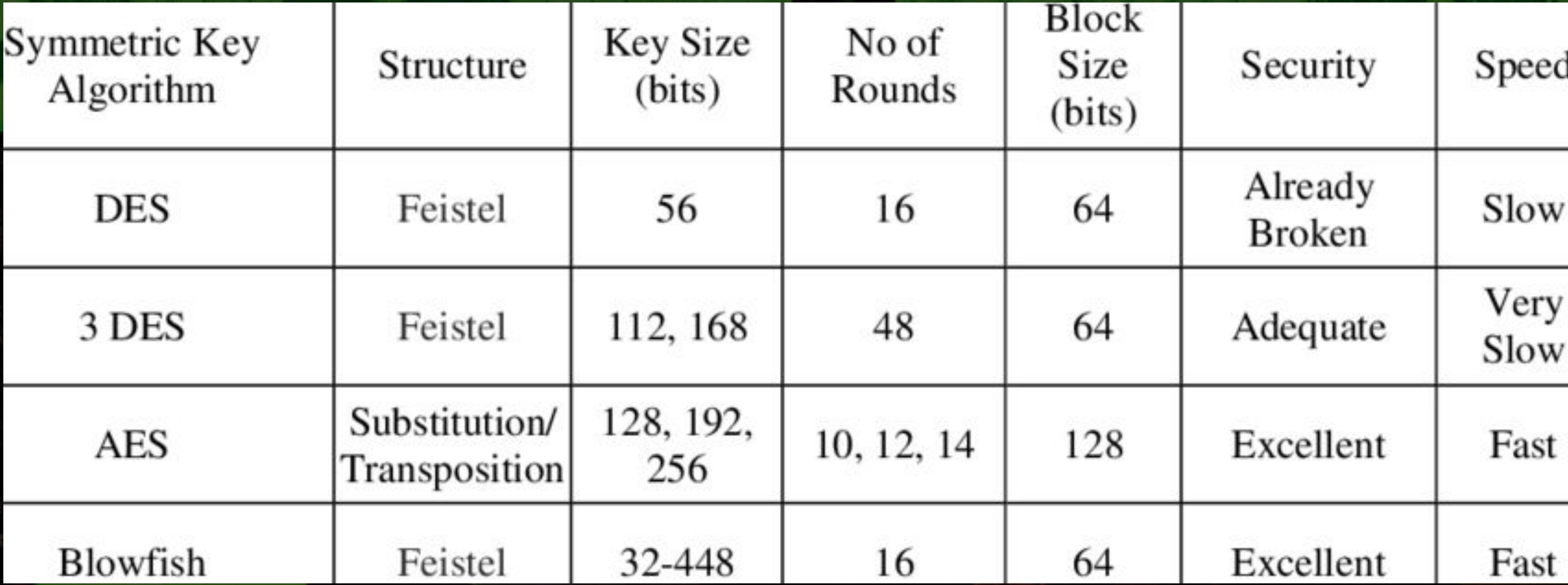
DES – “Data Encryption Standard”

Most influential encryption scheme for modern cryptography.

“Developed in the 1970’s at IBM and backed by the NSA for a delicious backdoor” – basically from the wiki

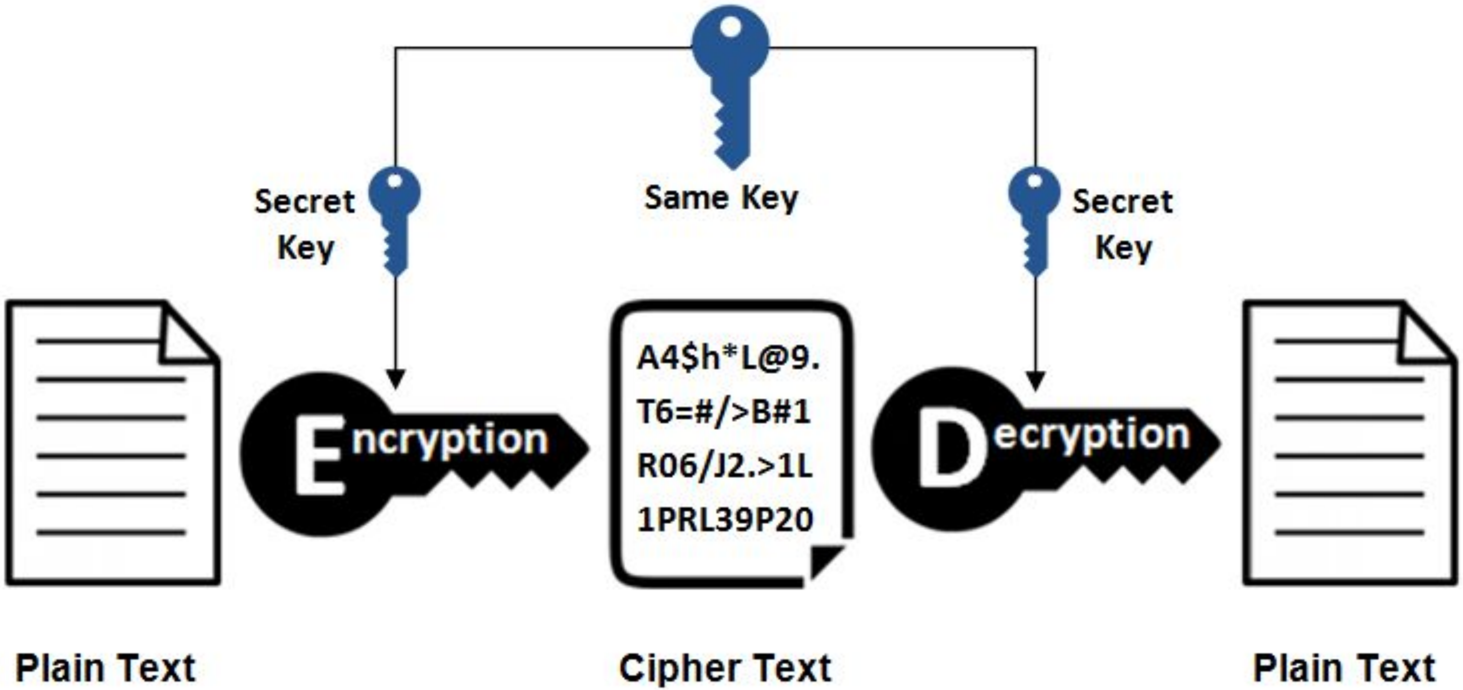


Modern form of DES - (AES)



Symmetric Key Algorithm	Structure	Key Size (bits)	No of Rounds	Block Size (bits)	Security	Speed
DES	Feistel	56	16	64	Already Broken	Slow
3 DES	Feistel	112, 168	48	64	Adequate	Very Slow
AES	Substitution/ Transposition	128, 192, 256	10, 12, 14	128	Excellent	Fast
Blowfish	Feistel	32-448	16	64	Excellent	Fast

Symmetric Encryption



Same Key

Secret Key

Secret Key

Encryption

Decryption

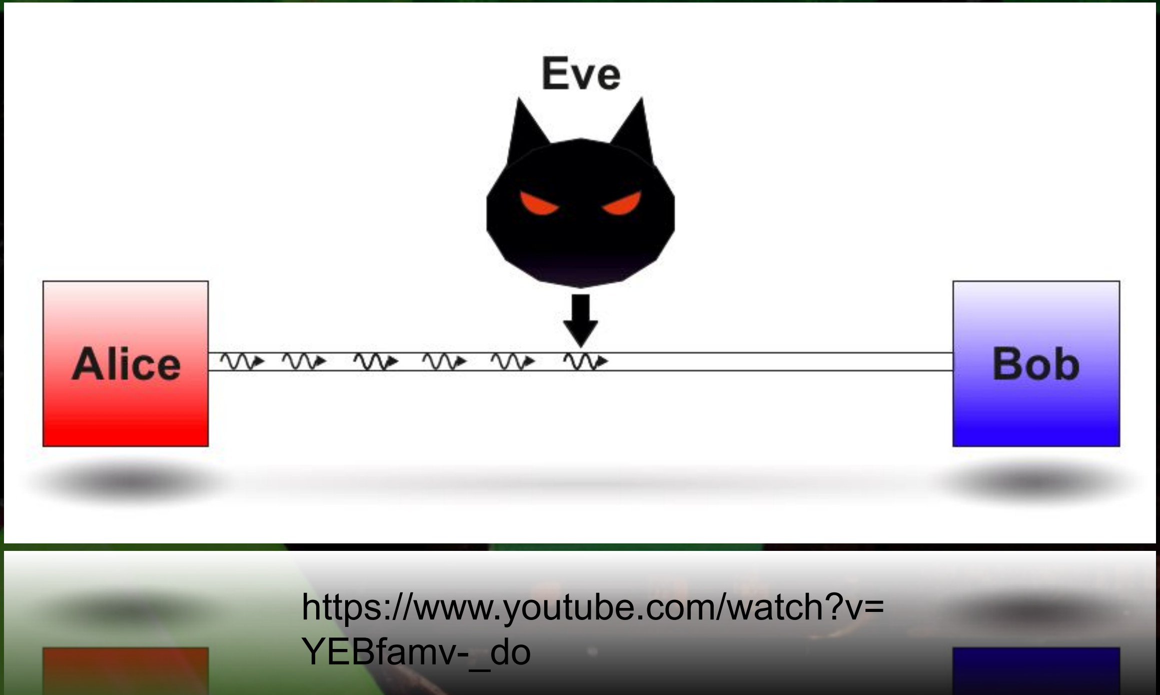
A4$h*L@9.
T6=#/>B#1
R06/J2.>1L
1PRL39P20

Plain Text

Cipher Text

Plain Text

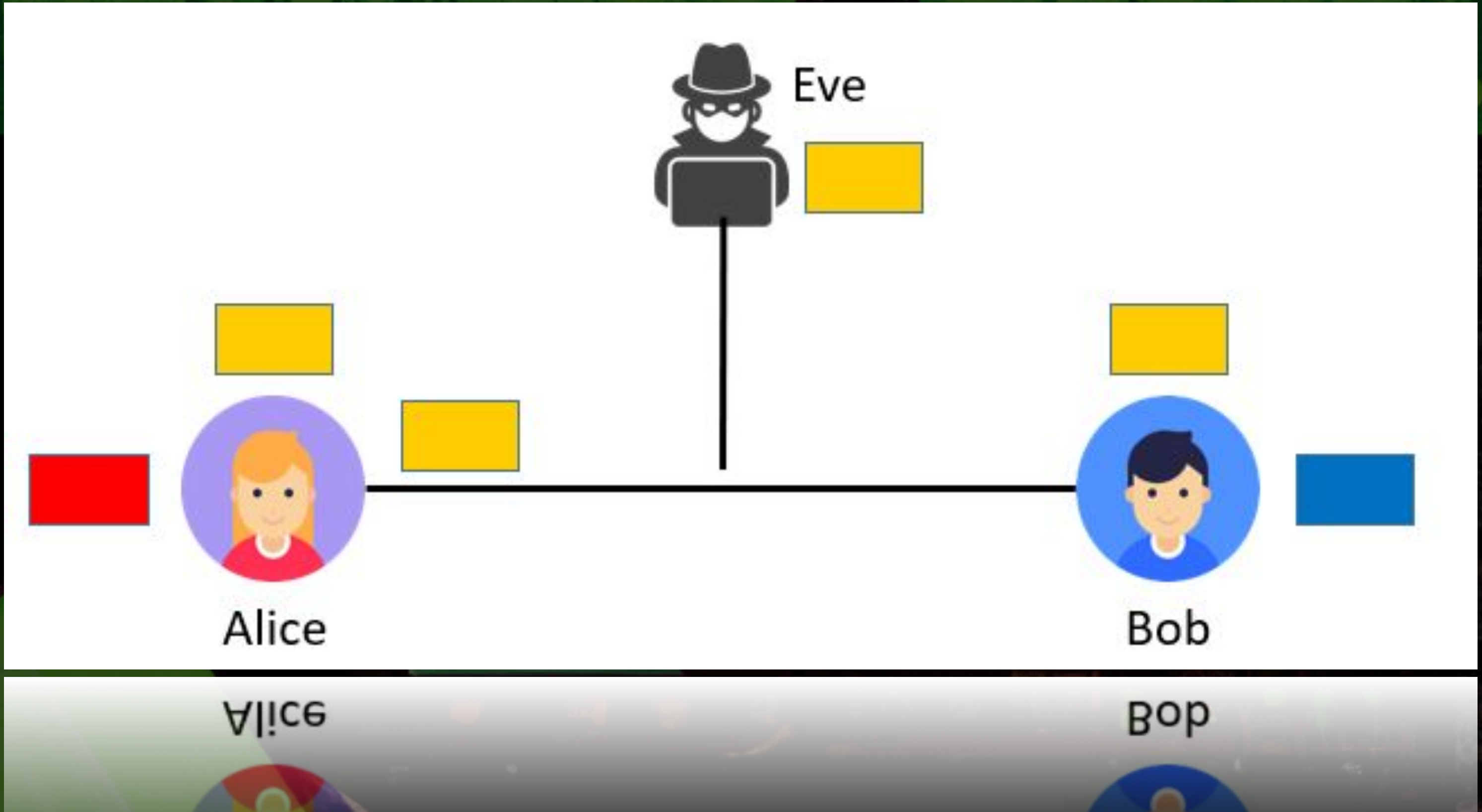
Asymmetric keys are special because they try to solve the problem of key distribution and power the world of the internet.

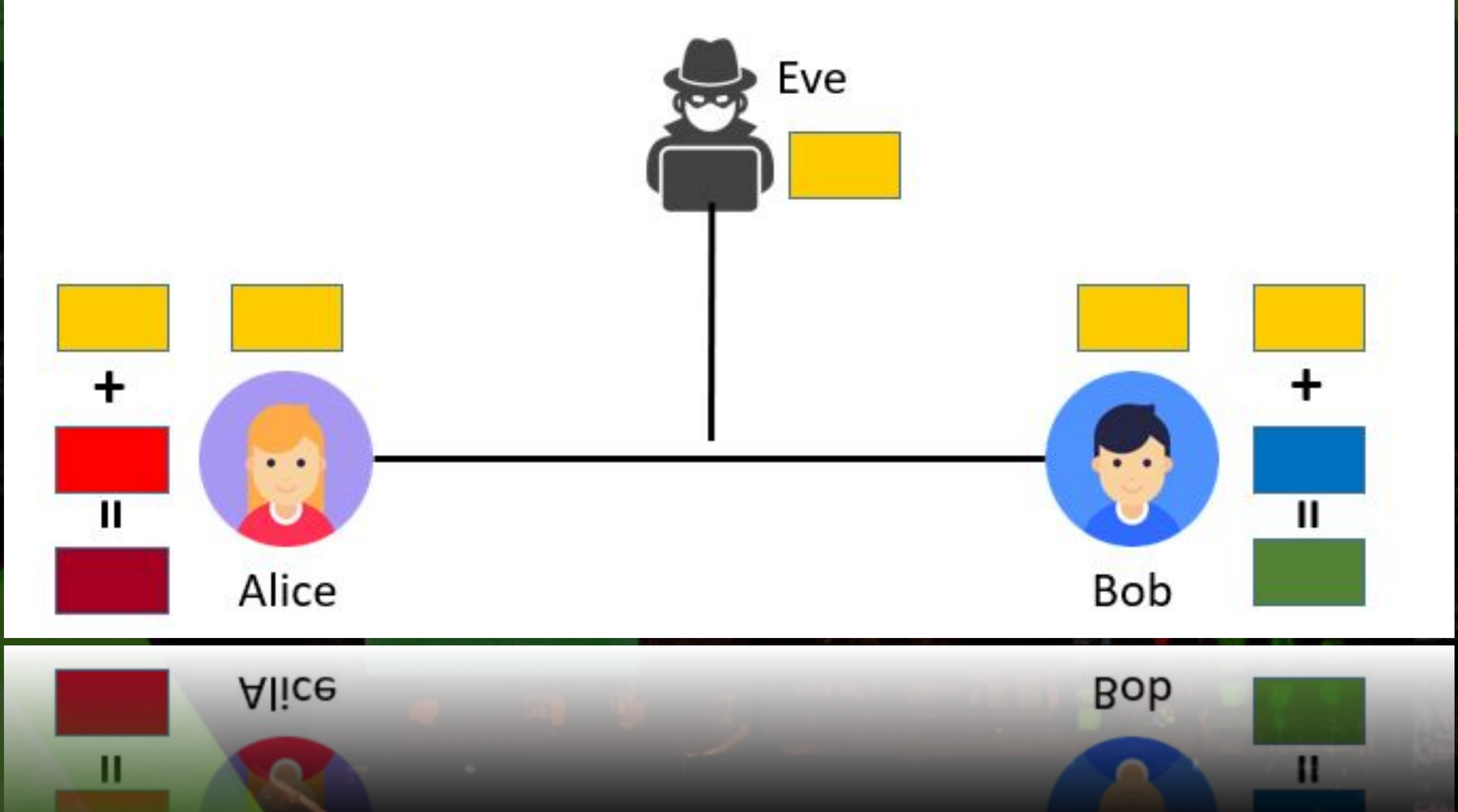


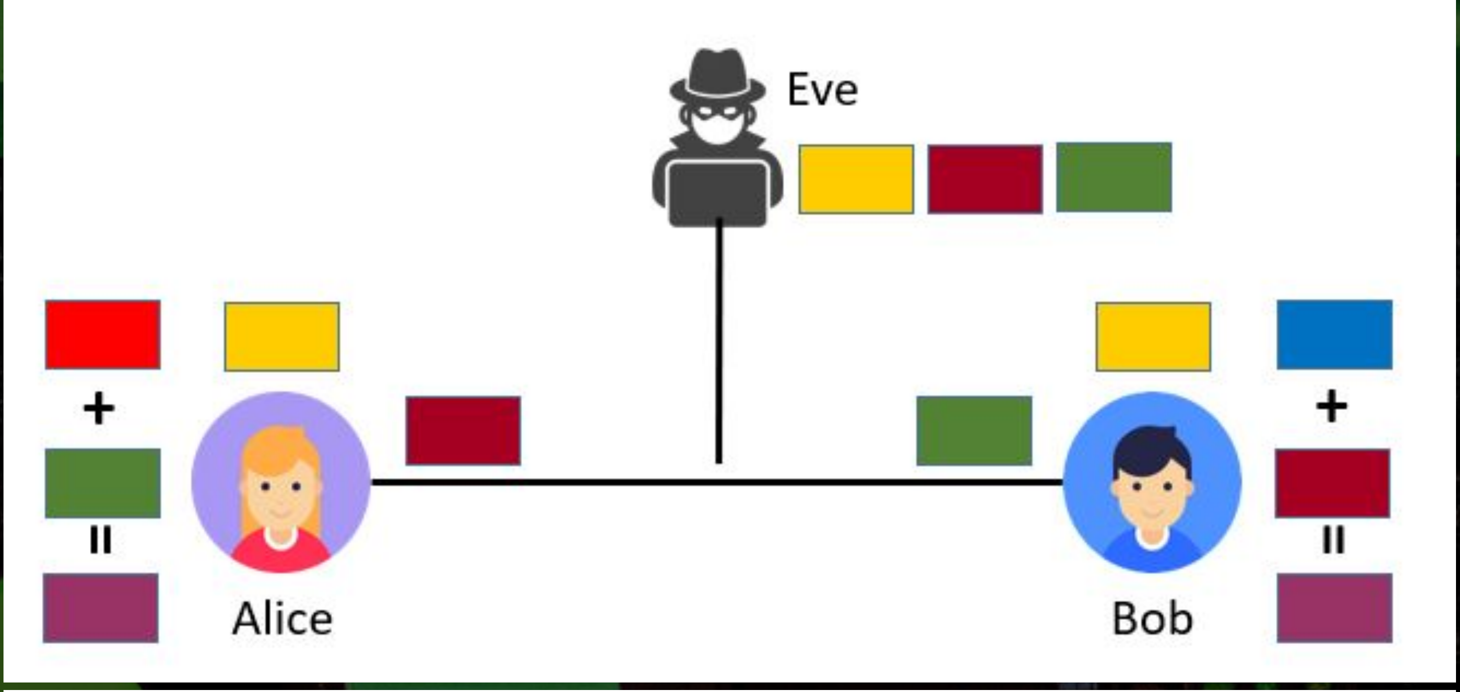
https://www.youtube.com/watch?v=YEBfamv-_do

Assume Bob and Alice want to share a key to initiate an encrypted communication. How can they do this while Eve - I mean Oskar - is always listening?

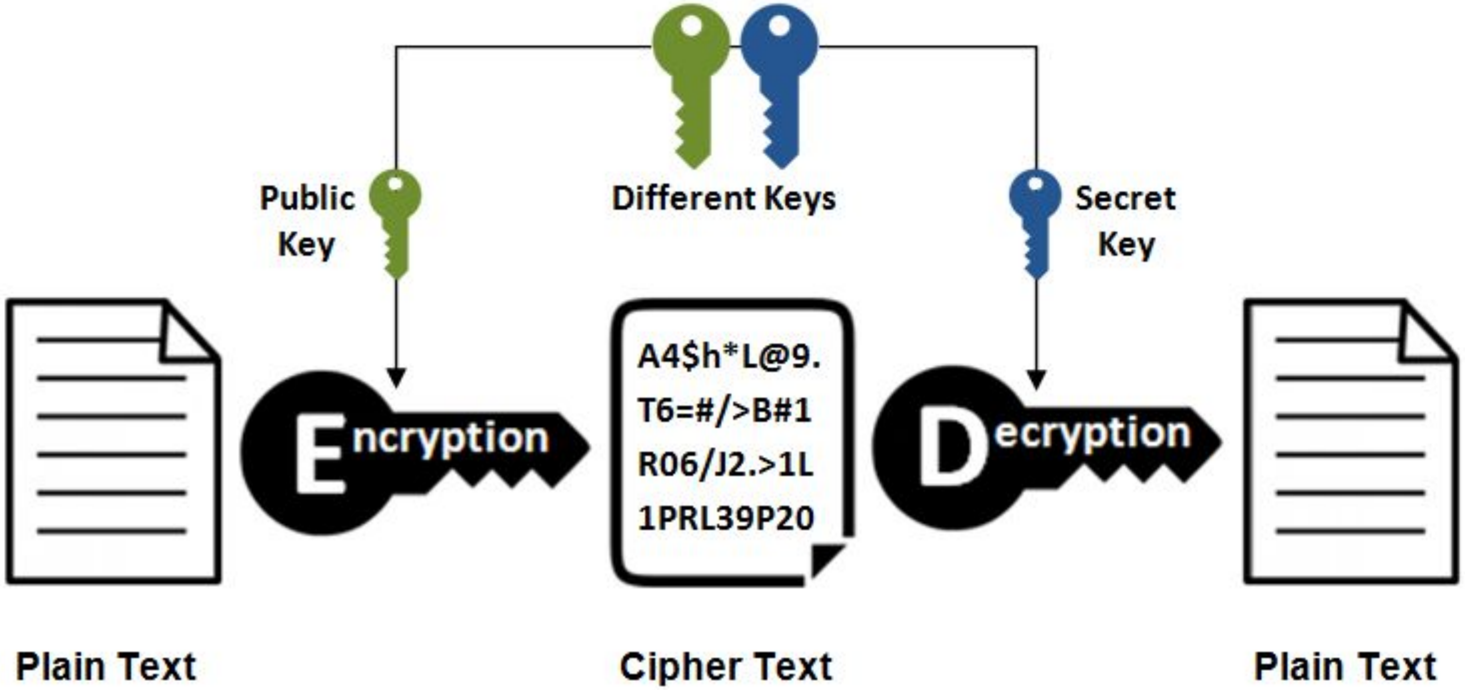
Let’s look at a quick example using some intuition.




Eve
+
=
Alice
+
=
Bob


Eve
Alice
Bob
+
=
+
=

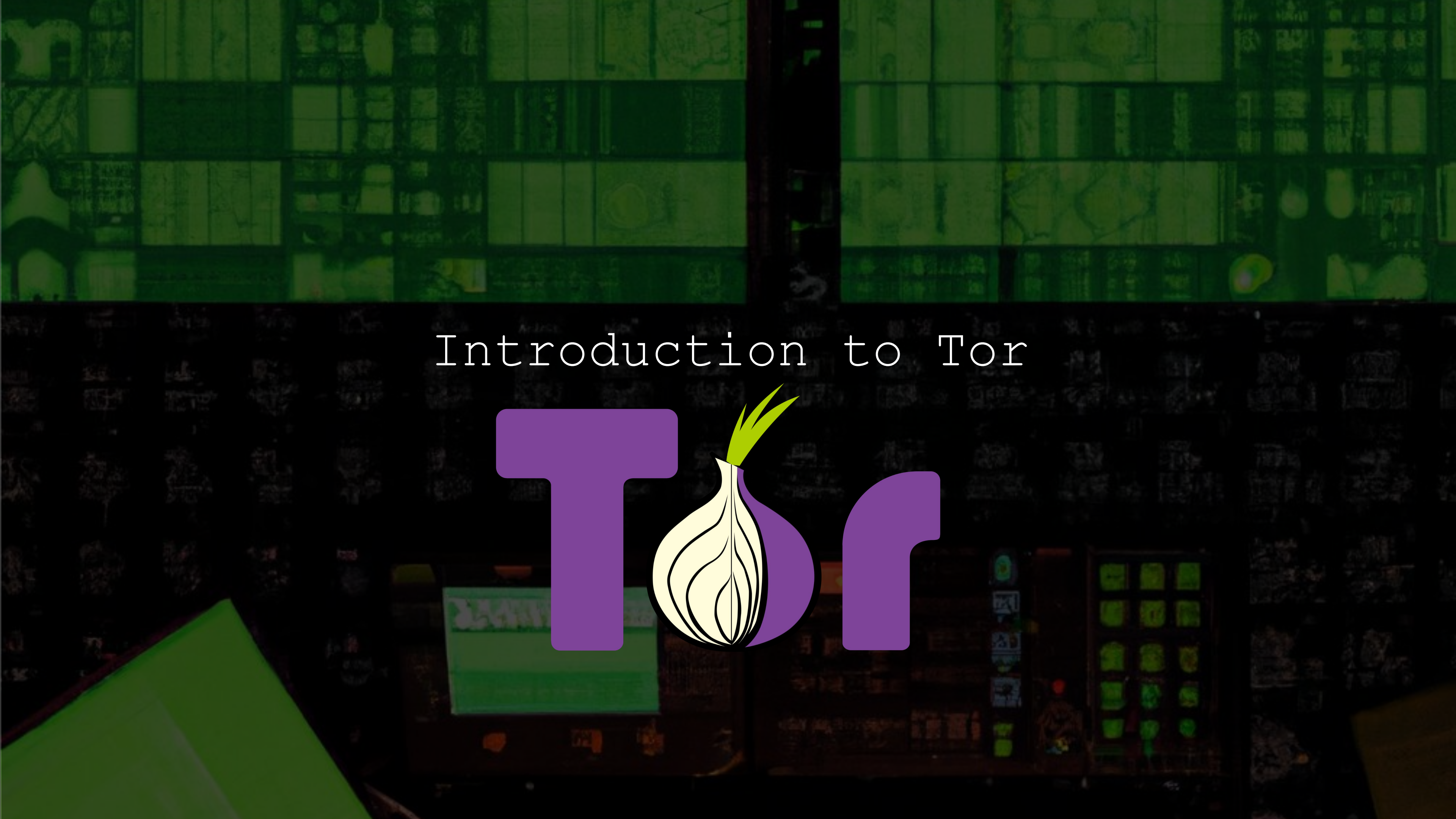
Asymmetric Encryption



Optional RSA video to watch (Very Interesting) (Builds off Diffie-Hellman)(Powers internet!)

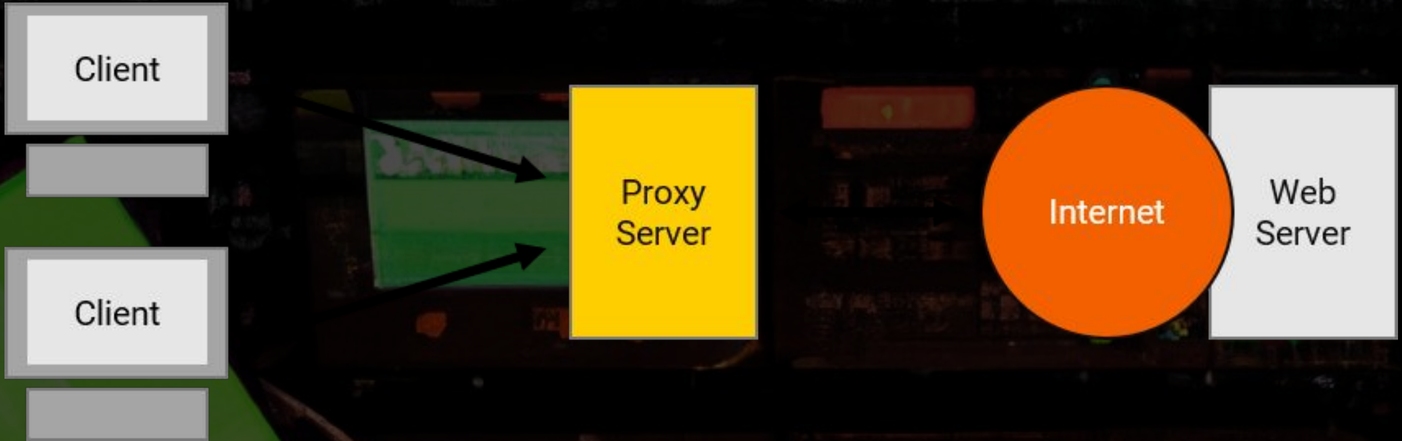
Public Key Cryptography: RSA Encryption Algorithm

Introduction to Tor

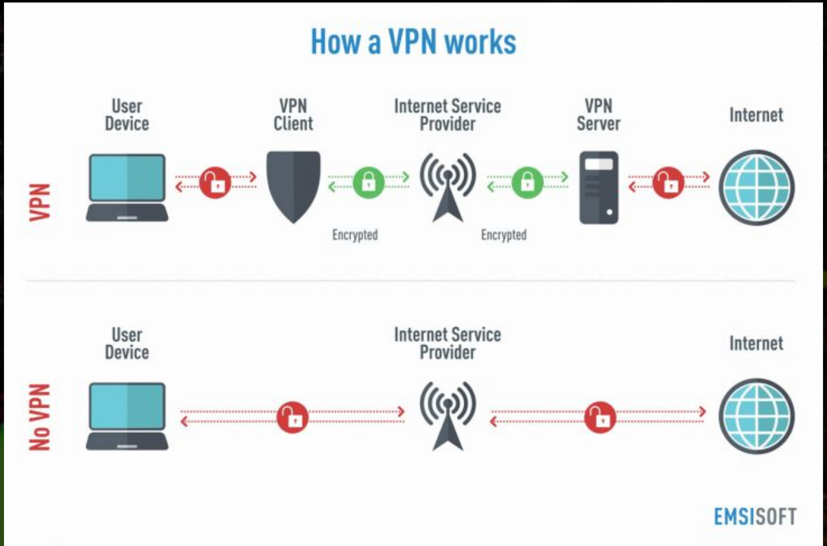


What is a proxy? What is a VPN.

A proxy server (in this context) is used to act as a “middleman” between your connection to another server. Instead of eavesdropping on your conversation (sussy), it masks the client’s identity when connecting to a server.

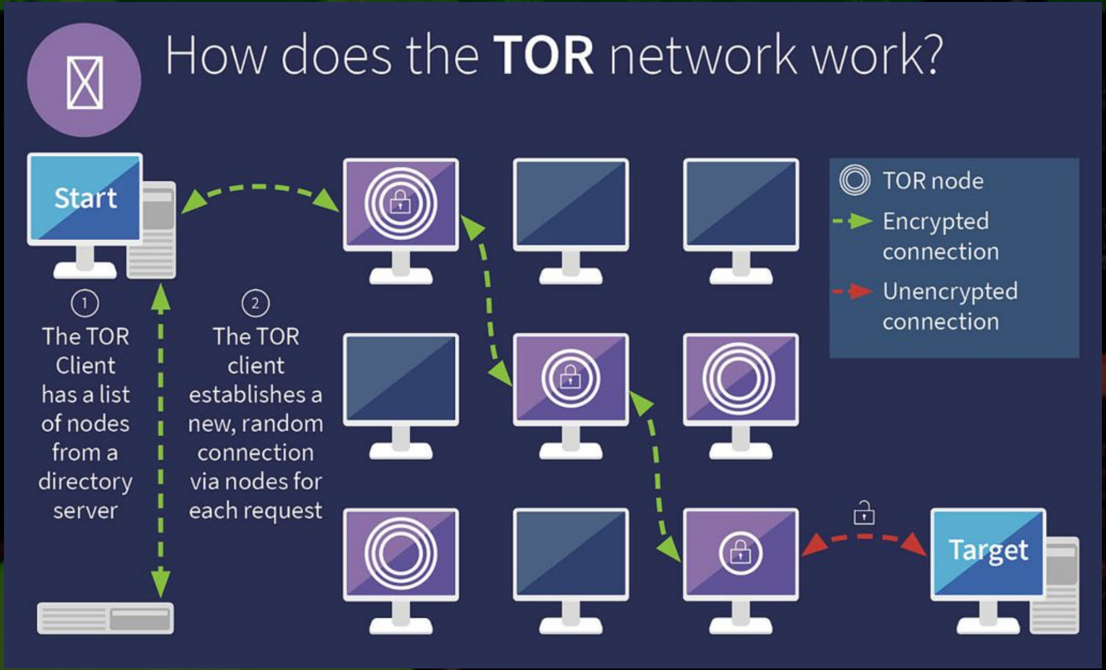


A VPN builds on top of an idea of a proxy but provides extra services to encrypt and hide the identity of the user. Companies that offer these services love to boast about “complete privacy” and all that noise.



Free alternative, Tor

Tor uses multiple relay nodes (proxies) in an attempt to completely randomize and anonymize your identity.



How does the **TOR** network work?

Start

1 The TOR Client has a list of nodes from a directory server

2 The TOR client establishes a new, random connection via nodes for each request

Target

◎ TOR node

🟩 Encrypted connection

🟥 Unencrypted connection

Tor **anonymizes** your connection, but that does not necessarily mean that its **private**.

Because of the many hops and computations that relay nodes have to perform to keep your traffic secure, tor is often very slow.

Anyone can host a tor node, provided that they follow the standard protocol for being a node - remember the Kerckhoff Principle. However, it seems as though authentication can be attacked.

https://nusenu.medium.com/is-kax17-performing-de-anonymization-attacks-against-tor-users-42e566defce8

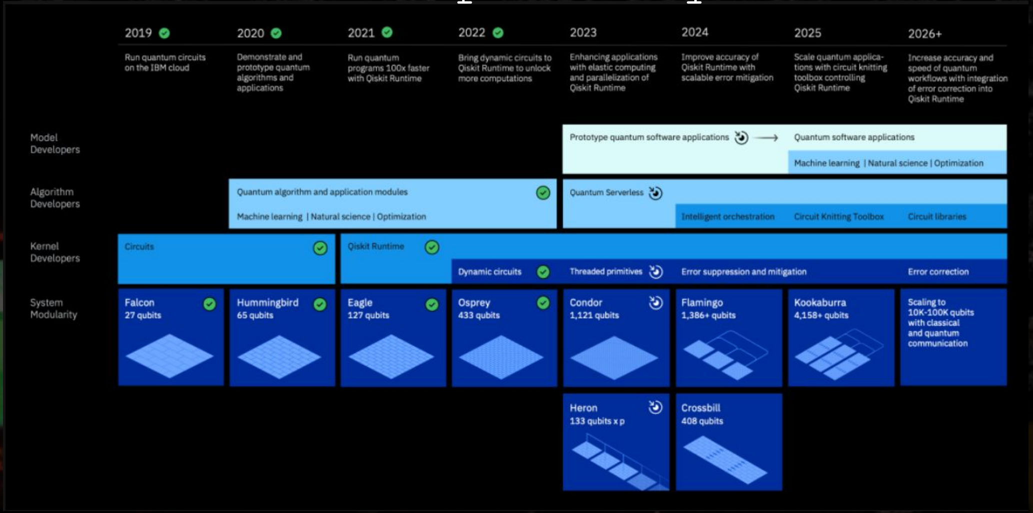
Most* of these encryptions are resistant to classical brute force attacks - but in the quantum world everything is different.

Green Glow
Protein Smoothie

GF | DF | LC | MP | Q

Kcal	Fats(g)	Carbs(g)	Protein(g)
102	6	4	10

IBM’s roadmap for quantum



2019 ✓
Run quantum circuits on the IBM cloud

2020 ✓
Demonstrate and prototype quantum algorithms and applications

2021 ✓
Run quantum programs 100x faster with Qiskit Runtime

2022 ✓
Bring dynamic circuits to Qiskit Runtime to unlock more computations

2023
Enhancing applications with elastic computing and parallelization of Qiskit Runtime

2024
Improve accuracy of Qiskit Runtime with scalable error mitigation

2025
Scale quantum applications with circuit knitting toolbox controlling Qiskit Runtime

2026+
Increase accuracy and speed of quantum workflows with integration of error correction into Qiskit Runtime

Model Developers
Prototype quantum software applications → Quantum software applications
Machine learning | Natural science | Optimization

Algorithm Developers
Quantum algorithm and application modules ✓
Machine learning | Natural science | Optimization
Quantum Serverless
Intelligent orchestration
Circuit Knitting Toolbox
Circuit libraries

Kernel Developers
Circuits ✓
Qiskit Runtime ✓
Dynamic circuits ✓
Threaded primitives
Error suppression and mitigation
Error correction

System Modularity
Falcon 27 qubits ✓
Hummingbird 65 qubits ✓
Eagle 127 qubits ✓
Osprey 433 qubits ✓
Condor 1,121 qubits
Flamingo 1,386+ qubits
Kookaburra 4,158+ qubits
Scaling to 10K-100K qubits with classical and quantum communication
Heron 133 qubits x p
Crossbill 408 qubits

Arguing that you don't care about privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.

Who wants your delicious data? Spooky season edition🎃

https://www.wired.com/2013/09/nsa-backdoor/

Having your data exposed is inevitable, but you can make it harder for the ones who want it.

- Use software that provides encrypted and serverless communications. (Notable - Signal)
- Don’t fully rely on commercial proxies or VPNs to mask your identity. Make use of decentralized anonymous proxies (Tor)
- Use software that helps disrupt advertisement tracking when using your browser. (AdNauseam, vtoubiana/TrackMeNot, NewPipe)
- Paranoia edition - Live in the woods

Trying to get a more-in-depth look into cryptography? Look no further.

https://cryptopals.com/

Secret resources in the github

Math (Number Theory, Combinatorics, Abstract Algebra, Tequila)