Today

Intro to cryptography

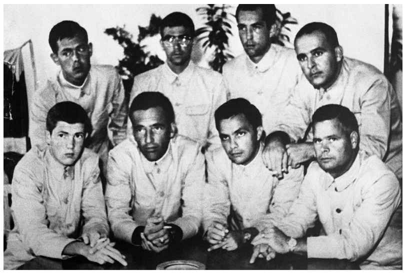
Classical cryptography

Κρυπτογραφία (cryptography)

κρυπτός: hidden, secret

γράφειν: writing

- in general: transforming a *message* using *secret knowledge*
- in more technical terms: *plaintext* ⇄ *ciphertext* using a *key**



* Not *all* cryptograhic operations require a key, but we'll start with those that do.

This famous photograph of US POWs in North Korea is an example of something that bears a hidden meaning to those with secret (or at least not-ubiquitous) knowledge. This photo was staged to show how happy captured US sailors were supposed to be in their new homes, but there is a hidden digital message...

Security goals

Confidentiality	Encryption
Integrity	MACs, signatures
~~Availability~~	
Authentication	Password hashing
~~Authorization~~	
~~Accountability~~	

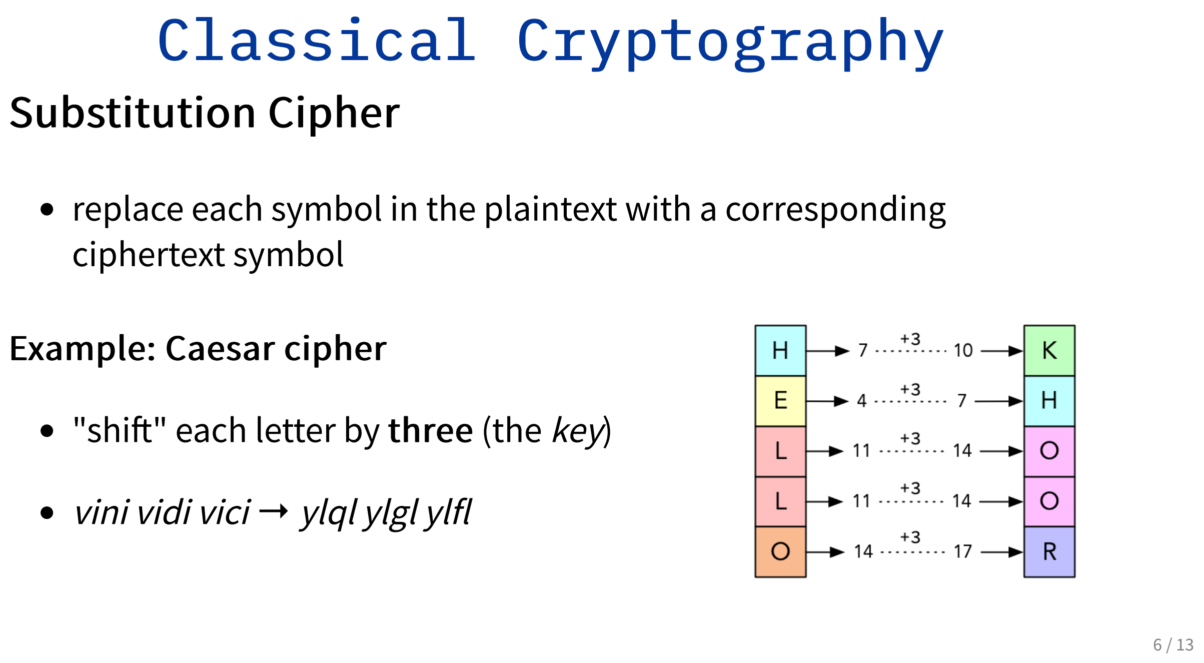
Cryptography is a useful tool... but it's *just* a tool

Cryptography is a useful mechanism that can be _____________________________ that achieves security goals.

As Peter Neumann said:

> *If you think cryptography is the answer to your problem, then you don't know what your problem is.*

Cryptography doesn't solve problems by itself. Encrypting a network packet doesn't secure the hosts doing the communication. Putting a contract on a blockchain won't stop people from breaking their word. A secure system is much more than just cryptography. However, cryptography is an important *part* of most secure systems.



Classical Cryptography

Substitution Cipher

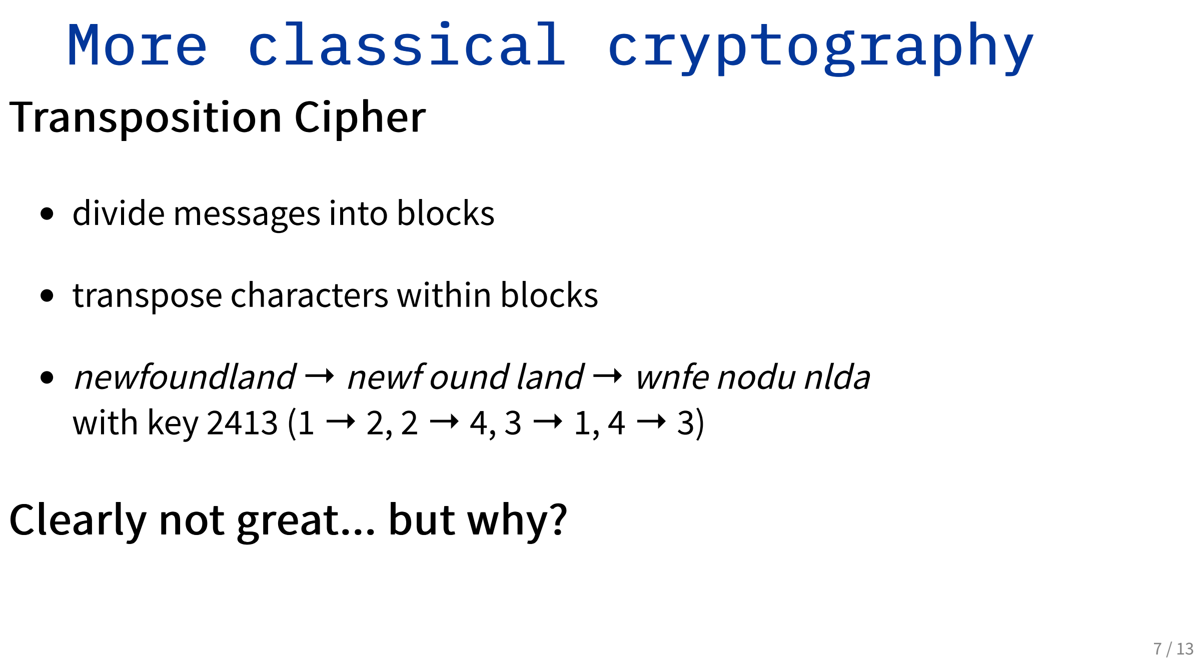
- replace each symbol in the plaintext with a corresponding ciphertext symbol

Example: Caesar cipher

- "shift" each letter by **three** (the *key*)
- *vini vidi vici* → *ylql ylgl ylfl*

Classical cryptography refers to everything from the classical era (hence the Greek name!) up to the 20th Century. *Modern cryptography* is based on mathematical problems like the discrete logarithm problem — we'll talk about such things we get to public-key cryptography. In between, there's some awkwardness where different experts may disagree on definitions. Modern block ciphers aren't modern enough for some people, but they're definititely not classical either.

I would suggest that you think of classical cryptography as ______________________ ______________ (very broadly defined) and modern cryptography as ______________________ ____. However, don't be surprised if you encounter someone who doesn't think that definition is "pure" enough. 😉



More classical cryptography

Transposition Cipher

- divide messages into blocks
- transpose characters within blocks
- *newfoundland* → *newf ound land* → *wnfe nodu nlda*
  with key 2413 (1 → 2, 2 → 4, 3 → 1, 4 → 3)

Clearly not great... but why?

If you don't know the key to such a transposition cipher, what might you try in order to find it?

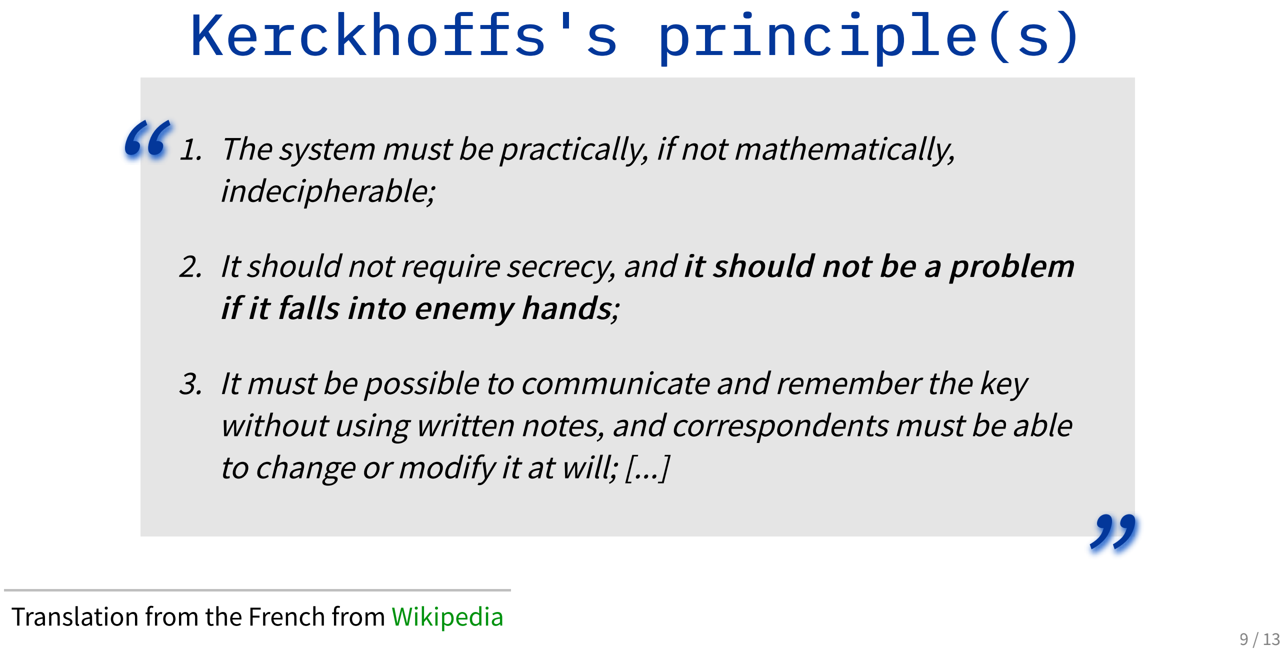
Cryptanalysis

- given some plaintext and/or ciphertext, find the key
- find a fatal flaw ("break") that subverts a cryptosystem

Most fundamental example: exhaustive key search

- given some ciphertext (*ylql ylgl ylfl*), try all possible key values
- 1 → *xkpk xkek xkek*, 2 → *wjoj wjej wjdj*, 3 → *vini vidi vici*
- possible if correct plaintext is **distinguishable**, easy if some P/C pairs are known (yes, this is actually possible!)

It might seem unlikely that an attacker would have access to all details of the system, plus plaintext and ciphertext pairs, but it's actually not. In WWII, British codebreaking was sometimes aided by feeding specific plaintexts to the German enemy via a process called "gardening") (laying sea mines in specific locations to create minesweeping messages).



Kerckhoffs's principle(s)

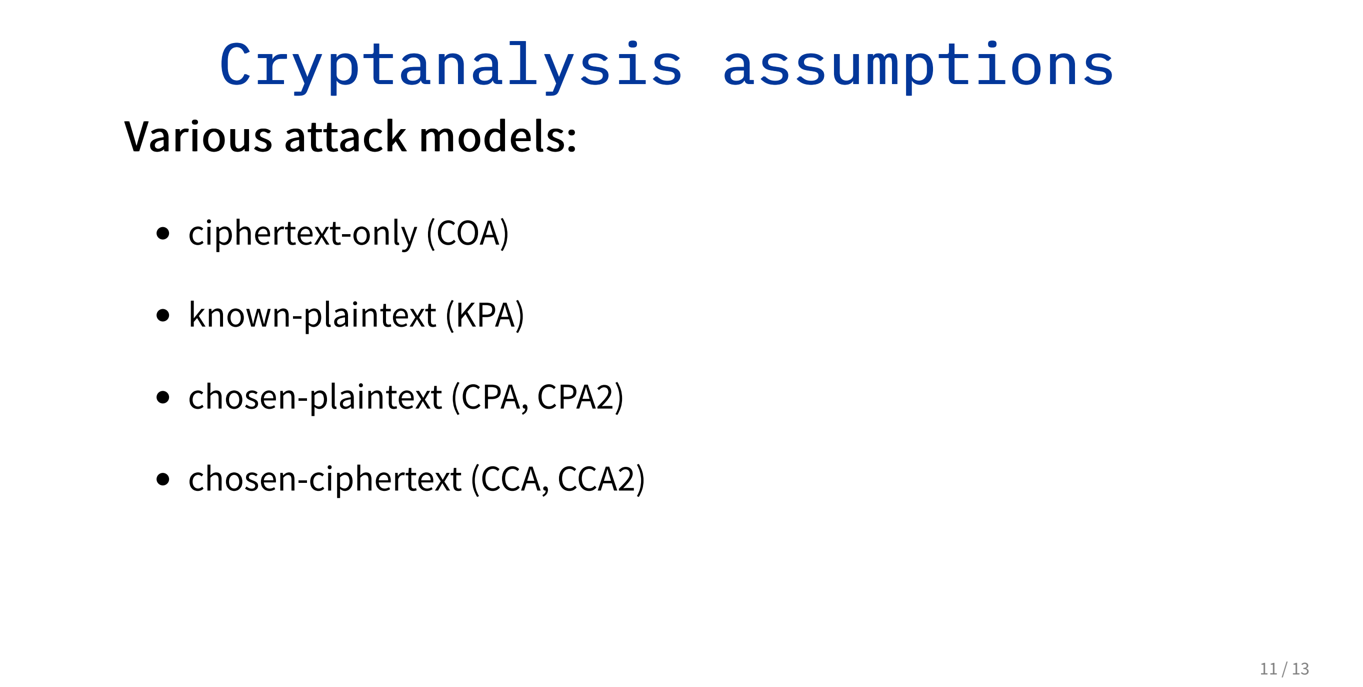
> 1. *The system must be practically, if not mathematically, indecipherable;*
> 2. *It should not require secrecy, and **it should not be a problem if it falls into enemy hands;***
> 3. *It must be possible to communicate and remember the key without using written notes, and correspondents must be able to change or modify it at will; [...]*

Translation from the French from Wikipedia

Kerchoffs had six principles, including that "it must be applicable to telegraph communications", but we're less interested in those. One key principle that we *are* still interested in is the second one: the security of a system ______________________ ________________________________. This is commonly mis-stated as, "the design should be public", but that's not quite what Kerchoffs said. Rather, the principle is that your security shouldn't ________________________________.

Exhaustive key search

- Caesar-style *shift cipher*: 26 possible keys (well, really 25)
- Modern AES-128 cipher: 2^{128} keys — could take awhile!
  - 10,000 CPUs checking one key / ns
  - $10^4\,\mathrm{CPU} \times 10^9\,\frac{\mathrm{key}}{\mathrm{CPU}\cdot s} \times 10^{4.9}\,\frac{s}{d} = 10^{17.9}\,\frac{\mathrm{key}}{d} = 2^{59.5}\,\frac{\mathrm{key}}{d}$
  - need $2^{67.5}$ days, i.e., 209 Edays / 572 Pyears / 63.5 Msols
- Lesson: make the key space large!



Cryptanalysis assumptions

Various attack models:

- ciphertext-only (COA)
- known-plaintext (KPA)
- chosen-plaintext (CPA, CPA2)
- chosen-ciphertext (CCA, CCA2)

In a ciphertext-only attack, the adversary can break your cryptosystem ______________________ ______________. This is the ________________________________, so to say that a cryptosystem can withstand it _______________________________.

In a known-plaintext attack, the adversary is assumed to __________________ _____________________________.

In a chosen-plaintext attack, the adversary is assumed to _______________________________ ______________________________ (like "gardening" in WWII, but much more direct / less costly).

Finally, in a chosen-ciphertext attack, the adversary is assumed to _______________________ ____________________________________.

Frequency analysis

Example of a ciphertext-only attack

- don't know the plaintext
- know something *about* the plaintext: symbol frequencies
- English: 12% e, 9% t, etc., common groupings: the, an, qu...

Exercise: decode shift-enciphered ciphertext via frequency analysis

hijstcih hdbtixbth tcrdst pcs strdst bthhpvth