Breaking Codes and Finding Patterns - Susan Holmes

<https://www.youtube.com/watch?v=oW69Zi152Nc&t=1715s>

Substitution Ciphers

Ciphering Permutation - (26! ≈ 288.4, or about 88 bits, = 4.03291461127e+26)

Frequency of the different letters -> English Language Frequency

1550’s

De Furtivis Literarum notis, vulgo de Ziferis libri IIII

by Giambattista Della Porta

<https://archive.org/details/bub_gb_sc-Zaq8_jFIC/page/n109/mode/2up>

De Vigenère Code - le chiffrage indéchiffrable (French for 'the indecipherable cipher').

<https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher>

Cryptanalysis - De Vigenère Code

<https://en.wikipedia.org/wiki/Kasiski_examination>

1922’s

<https://en.wikipedia.org/wiki/Index_of_coincidence>

<https://en.wikipedia.org/wiki/William_F._Friedman>

It’s called invariant

<https://en.wikipedia.org/wiki/Invariant_(mathematics)>

Status report – 1930’s

* Substitution ciphers: many possibilities (26! ≈ 288.4, or about 88 bits) easy to break
* Polyalphabetic ciphers like de Vigenère codes flatten the language broken by Coincidence Index (CI)
* The most unbreakable code is a onetime pad: a dynamic de Vigenère with a never-ending random keyword.

Enigma Machine

15:30