***Notes on cryptanalysis of the Hill Cipher***

*Jeudi 25/02:*

Beginning of the lecture first done by Alina Matyukhina.

Intro:

So the basics of Hill cipher is the separation of the plain text in blocks of size *d*, and to multiply each block by the key which is a matrix *d x d*. As this cipher is linear, it is easy breakable.

Hill cipher:

The plain text space is defined by the set of ALL meaningful English strings of length multiple of an integer d. (the length of the blocks). Each characters belong to Z/26Z.

To encode and get the cipher text C we do C = K \* P (where K is the key and P the plaintext) the whole modulo 26.

To decode as the matrix K of the Key is invertible, we just get P = K^-1 \* C and modulo 26 again.

So if you intercept d^2 pair of C/P you can easily do a mapping and find the matrix K.

Note on brute force*:*

To do an exhaustive search on the whole space of matrix K, you need 26^(d²) matrix multiplication because for each letter of the alphabet you need to test a matrix that is of size *dxd* , and then chose those who are meaningful so O(d^3\*26^(d²). Work with ciphertext length = 1.27*d².*

Improvement of the brute force attack: