ElGamal

# Theoretical background

In cryptography, the **ElGamal** encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange. The system provides an additional layer of security by asymmetrically encrypting keys previously used for symmetric message encryption. It was described by Taher Elgamal in **1985**.

# The application

When is pressed:

* Encryption button:
* checks if plain text is lowercase.
* takes each character from the plain text, and looks it up in the encryption key, appending the result to the encrypted message (the message is initially empty)
* the encryption is done character-by-character: at each step, each character is encrypted and the resulting two values (alpha and beta) are represented as three individual coefficients which are then converted into text (similar to the RSA lecture: k = 1, l = 3). Thus, each character in the text to encrypt becomes six characters in the text to decrypt.
* Decryption button:
* checks if cipher text is lowercase.
* checks if cipher text is valid (has a length multiple of 6: 3 from alpha + 3 from beta), then we do the following:

-we split the text into pairs of 6 characters;

-every pair is split into pairs of 3 characters in order to achieve the alpha and beta pairs;

-for each alpha and beta pair, we decrypt the text using the accordingly function m = (alpha)^(-a)\* beta;

-we construct the deciphered text and show it on the form.