# Lab 3: Code Cracking

Part 0: Design (5 points)

Ceasar Cipher
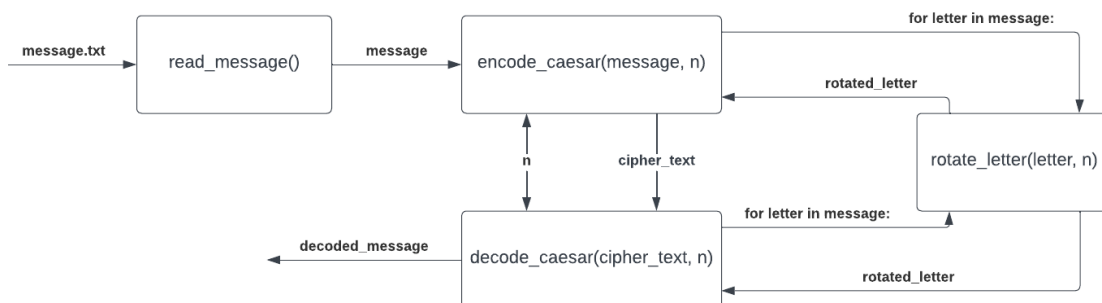
Vigenere Cipher
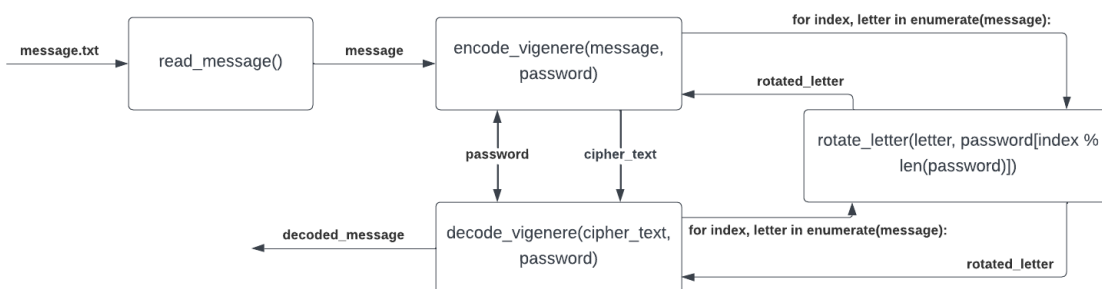
Encoding : encode_otp (message)

①

string_to_binary(string)   binary_to_binary_string(binary)

message
string
→
message
binary
numeric
(integer)
→
message
binary
string
(string)

why do we need
that?

②

key = ''.join[get_random_bit() for _ in range(len(message))]

⟶ key (random, len(message))
binary string (string)

↓ binary_string_to_binary(bin_string)

key
binary numeric
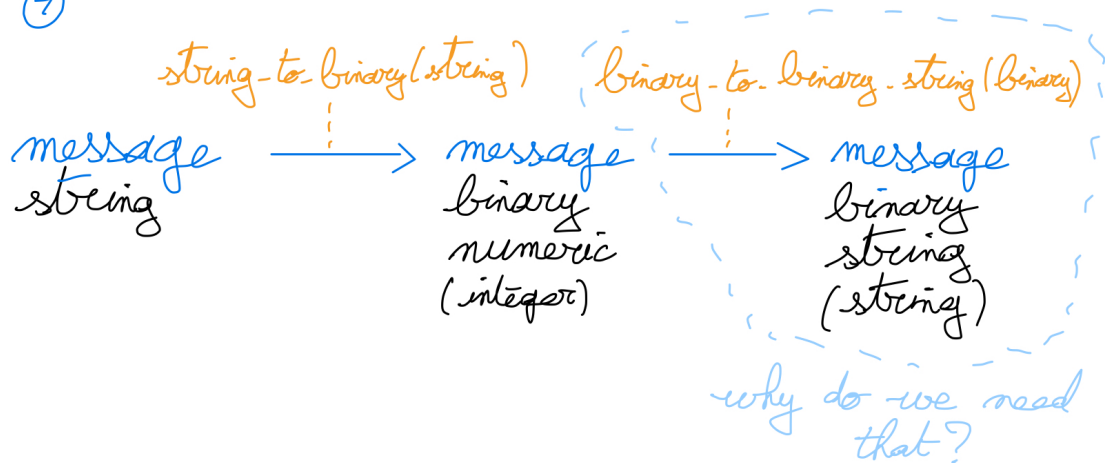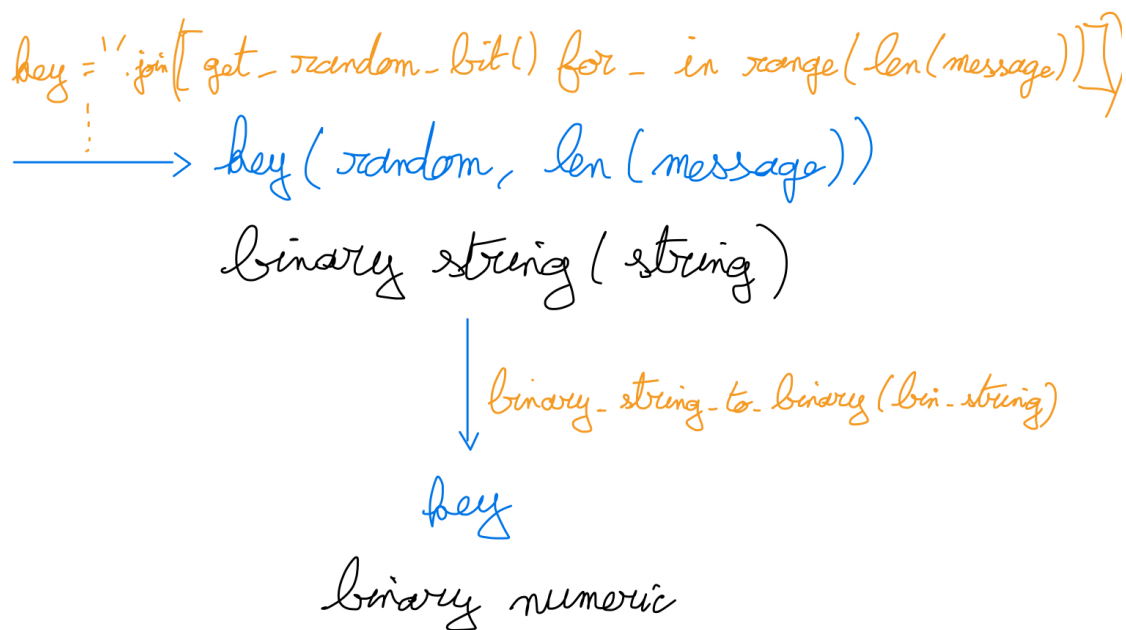
③ message XOR key
numeric   numeric

return cypher_text , key
       random number

Decoding : decode_otp (cypher_text, key)

cypher_text XOR key

↓

decoded_message
(binary numeric)

binary_to_string (n)

decoded_message
(string)