$$Pr[P = \text{"hello"} \mid C] \leftarrow$$

$$Pr[P = \text{"bye"} \mid C]$$

$$\vdots$$

Given a ciphertext seen by an adversary, it lists all the possible plaintexts and order them by decreasing probability. The plaintext with the highest probability is the most likely one.

In more details, we consider the probability that the plaintext has a given value conditionally to the ciphertext having the value seen by the adversary. The probability is taken over the possible keys.

Details of the derivation on slide 24 "The one-time pad".

We add p_i to both sides. Then, as we are computing mod 2, for any x, we have x + x mod 2 = 0, so we can simplify. Finally, the "o plus" notation indicates that we apply the same operation to all bit positions.

$$c_i = k_i + p_i \mod 2$$

$$c_i + p_i = k_i + p_i + p_i \mod 2$$

$$c_i + p_i = k_i$$

$$c \oplus p = k$$

Having seen this ciphertext:

$c = 001101$

We list the possible plaintexts. For each, we deduce the corresponding key and evaluate its probability.

$p = 000000$

$k = 001101$

$1/2^6$

$p = 011101$

$k = 010000$

$1/2^6$

$p = Ok!$

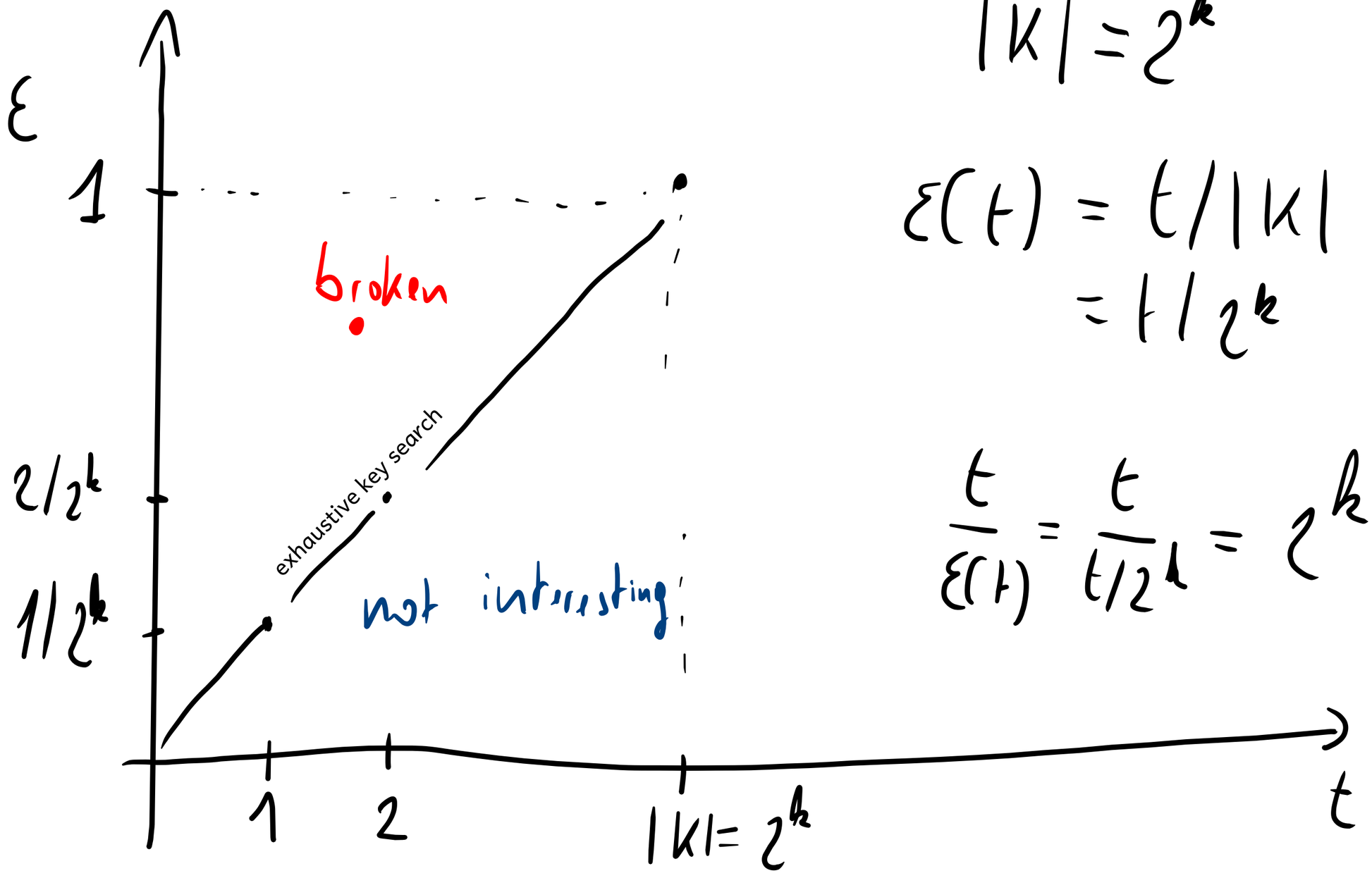
$p = yes$

$p = No!$

But they all have the same probability. How to deduce the right (or most likely) plaintext? We can't! This is unconditional security / perfect secrecy.

$$|K| = 2^k$$

$$\varepsilon(t) = t/|K| = t/2^k$$



$$\frac{t}{\varepsilon(t)} = \frac{t}{t/2^k} = 2^k$$

$$\frac{t}{\varepsilon} \geq 2^s$$

Details about slide 28 "Computational security".

The reason for considering t/ε is that an attack that takes time t and has a proability of success ε has to be repeated on average 1/ε times to have probability close to one.

$$\log_2 \frac{t}{\varepsilon} = \log_2 t - \log_2 \varepsilon \geq s$$