① Kámen-nůžky-papír vzdáleně, bez švindlu:

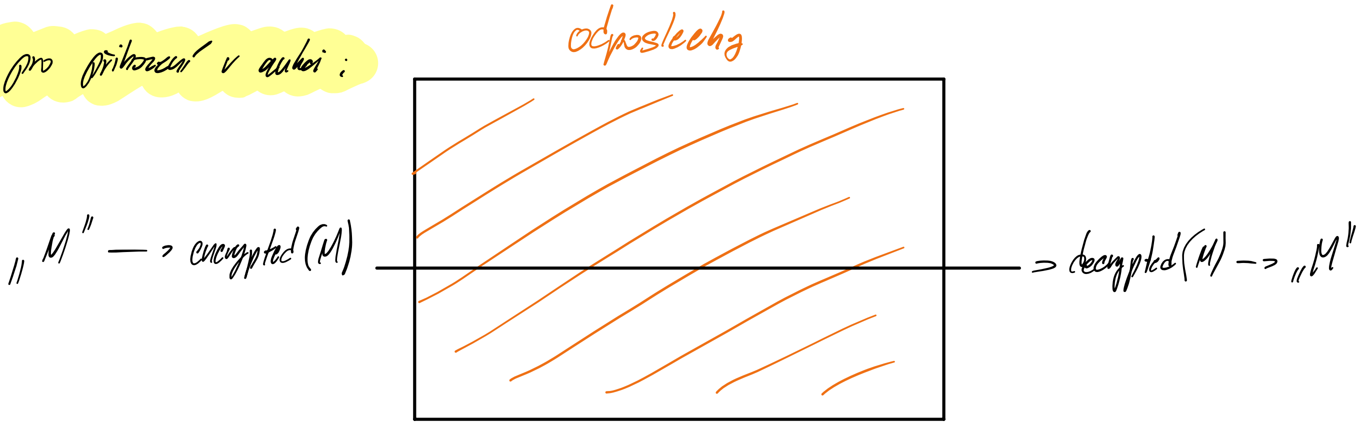
Jak odehrát, aby se nemohlo podvádět? (s hashovací funkcí)

Zahashujeme každý znak a plevel, pak si přímo řekneme, co jsme dali a jaký byl plevel, a pak znovu zahashujeme, co mi říkal protivník za znak a plevel a porovnáme hash, jestli opravdu říkal pravdu.

Pro minci:

- jak z dvou závislých hitů udělat nezávislý jev --> XOR --> není závislé, jestli budou obě T/F

② Protokol pro přihození v aukci:



- Kdyby tak furt posílal zašifrovaný stejný text, protivníci nebudou schopni dešifrovat, ale budou vědět, co po zprávě následuje, např.: přihoď

- přidám vždy náhodný plevel --> NONCE

- Reply-attack

- pošlu znovu nějakou starou zprávu (protože už vím, co po ní udělal)

+ proto se přidává unikátní id zprávy

- Padding

- jelikož ideální šifra zašifruje cokoliv, tak délka šifry odpovídá délce vstupu.
- proto musím zvětšit celkovou délku zprávy a do té budu paddovat zbytek, aby zpráva byla fixní.

③ Hashování hesel z webu

- sůl a pepř

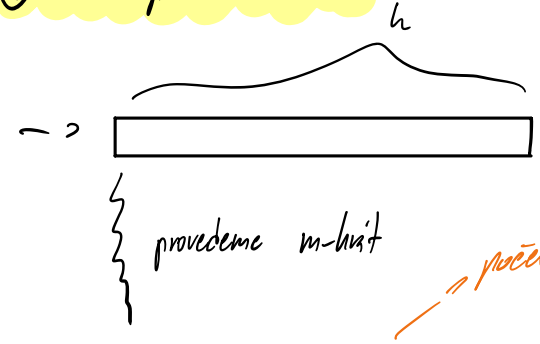
- pepř.: master klíč, který se přidává k heslu před hashováním
  - není součástí databáze, ideálně tak, aby zloděj nemohl zjistit

- sůl: unikátní kód ke každému uživateli, uložen jako plaintext v databázi
  - pak ke slovníkovému útoku by na každé slovo musel vyzkoušet všechny použité soli z databáze.

④ Pravděpodobnost kolize

Udělat to musíme pustit, aby byla šance shody byla $\geq 50\%$.

h-bitové číslo



2^h je to $2^{\frac{h}{2}}$

počet všech možností, kde jsme nemuseli kolizi

Nechť # možností vstupu h-bitového čísla $n = 2^h$

$$\frac{n \cdot (n-1) \cdot (n-2) \cdots (n-m+1)}{n^m} = 1 \cdot \left(1 - \frac{1}{2^h}\right) \cdot \left(1 - \frac{2}{2^h}\right) \cdots \left(1 - \frac{m-1}{2^h}\right)$$

počet všech možností

$$1 \cdot e^{-\frac{1}{2^h}} \cdot e^{-\frac{2}{2^h}} \cdots = e^{\frac{m \cdot (m-1)}{2^h}} = \frac{1}{2}$$

$$\frac{m \cdot (m-1)}{n} = \log_2(4)$$