① Kámen – nůžky – papír vzdáleně, bez švindlu:

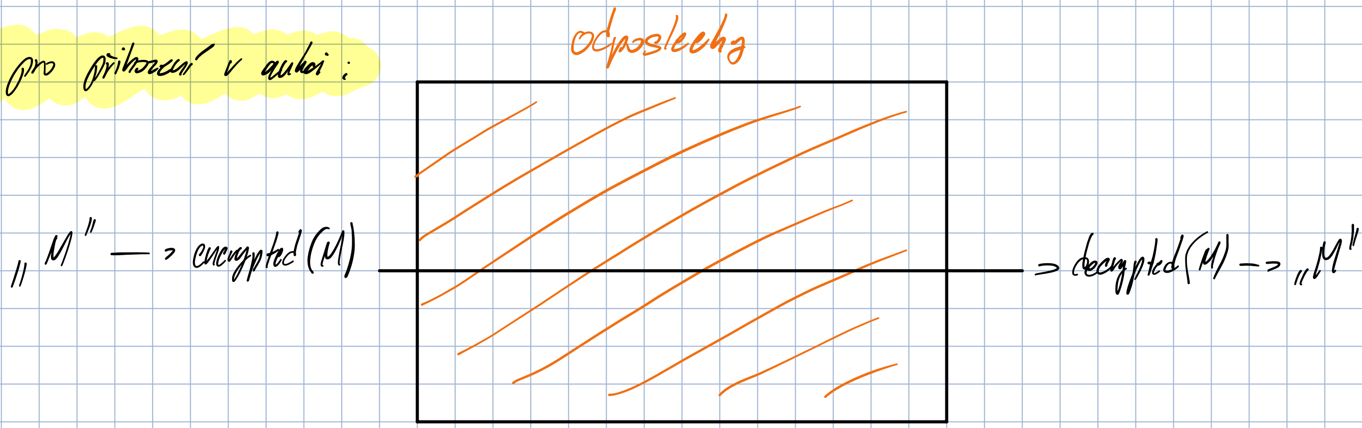
Jak odehrát, aby se nemohlo podvádět? (s hashovací funkcí)

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

Pro minci:

– jak z dvou závislých bitů udělat nezávislý jev --> XOR --> není závislé, jestli budou oba T/F

② Protokol pro přihazování v aukci:



– Kdybych furt posílal zašifrovaný stejný text, protivníci nebudou schopni dešifrovat, ale budou vědět, co po zprávě následuje, např.: příhoz

– přidám vždy náhodný pelmel --> $\boxed{\text{NONCE}}$

– 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 kód, 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

Kolikrát to musíme pustit, aby byla šance shody byla ≥ 50%.

k-bitové číslo

$\to ?\ \overbrace{\boxed{\qquad\qquad\qquad}}^{k}$

provedeme m-krát

$2^{\boxed{k}}$ je to $2^{\frac{k}{2}}$

počet všech možností, kde jsme neměli kolizi

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

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

počet všech možností

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

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