1. *Kámen-Nůžky-Papír po chatu:*
   Alice s Bobem se nemůžou dohodnout, na co půjdou do kina. Poraďte jim, jak si mohou bez pomoci někoho třetího dát kámen nůžky, když si můžou posílat pouze textové zprávy. Samozřejmě tak, aby měli oba jistotu, že ten druhý nepodváděl. Co kdyby si místo toho chtěli po chatu hodit korunou?

2. *Protokol pro přihazování v aukci:*
   Na vzdáleném místě se koná aukce, které se nemůžeme fyzicky účastnit. Proto máme na aukci svého zástupce, ten umí přijímat pouze příkazy „přihoď“ a „nepřihazuj“. Z aukce existuje jednosměrný přímý přenos, můžeme tedy v reálném čase sledovat, co se právě draží a kdo kolik přihodil. Naše instrukce ale musíme zástupci posílat skrze komunikační kanál, který nemáme plně pod kontrolou, čehož by rádi využili naši soupeři v aukci. Vymyslete komunikační protokol pro tuto příležitost. Můžete předpokládat, že máte k dispozici kvalitní symetrickou šifru a váš zástupce zná tajný klíč.

3. *Hashování hesel:*
   Představme si webovou stránku, kam se uživatelé přihlašují pomocí jména a hesla. Aby hesla nemusela být na serveru uložena jako prostý text, který si může kdokoli přečíst, bývá zvykem na serveru ukládat pouze hashe hesel. Ve chvíli, kdy se uživatel chce přihlásit, pošle na server heslo. Na serveru je z tohoto hesla spočítán hash a porovnán s uloženým záznamem. Pokud jsou stejné, uživatel zadal nejspíš správné heslo a je přihlášen.

   Hashování hesel je určitě vhodným postupem. Pokud ale jednoduše spočítáme hash z hesla, stále můžeme při odcizení hashů čelit určitým rizikům. Napadá vás, kde jsou nedostatky takového postupu? Dokážete najít a popsat, jak ukládat hesla lépe?

4. *Pravděpodobnost kolize (bonusová úloha):*
   Představme si ideální hashovací funkci, která má výstup o velikosti k bitů. Kolik (asymptoticky) výpočtů hashovací funkce budeme muset provést, abychom s pravděpodobností alespoň 50 % našli dvě hodnoty se stejným hashem?