### Úlohy na precvičenie – KRS 2023 – séria I

Úlohy riešte samostatne a podrobne. Celý postup zaznamenajte a komentujte. Odpovedajte na položené otázky. Odpovede zdôvodňujte celými vetami. Na prvom liste uveďte svoje meno a zdroje, ktoré ste pri riešení použili. Za každé správne a vyčerpávajúce riešenie (samozrejme aj s postupom) v tejto sérii možno získať bod. Zlomky bodov možno získať aj za čiastočné riešenia. Riešenia tejto série je nutné doručiť do 20. 11. 2023, 15:20 (do začiatku prednášky). Pred týmto termínom je možné odovzdať riešenia na sekretariáte Ústavu informatiky (do môjho priečinka). Neskôr dodané riešenia a plagiáty nebudú opravované ani hodnotené. Problémy môžete konzultovať po prednáške alebo e-mailom na adrese jozef,jirasek at upjs sk.

1. Prístup do databázy chcem viazať na znalosť rodného čísla bez dátumu narodenia (štvorčíslia za dátumom). Odhadnite pravdepodobnosť, že v ročníku s 50 študentmi sa nájdu aspoň dvaja takí, ktorí majú toto štvorčíslie rovnaké (stačí odhad zo slajdu 5 z prednášky).

2. Ako možno využiť narodeninový paradox na zisťovanie diskrétneho logaritmu? Poznáme hodnotu y = gx mod p a chcem spočítať x, keď poznám p - veľké prvočíslo a g - generátor príslušnej cyklickej grupy. (návod – vypočítať gk mod p pre dostatočný počet náhodných čísel k a vypočítať tiež y.g-r mod p pre dostatočný počet čísel r ......). Popíšte podrobnejšie tento postup a odhadnite jeho zložitosť.

3. Uvažujme autentifikáciu hashovaciu funkciu Hn vytvorenú pomocou AES šifrovania so známym kľúčom K pre správu M1, M2, ... Mn takto: Hi = EK(Hi - 1 ⊕ Mi); H0 = 0. Ukážte, že to nie je dobrá kryptografická hashovacia funkcia (stačí pre dvojblokové správy – napr. pre zvolené A nájdite B, aby H2(A,B) = H2(M1, M2) – pre známu dvojblokovú správu M1, M2).

4. CBC-MAC hash (pre IV=0) jednoblokovej správy M je T. Aký bude CBC-MAC hash dvojblokovej správy M, M ⊕ T ?

\*. Ukázali sme, ako je možné použiť blokovú šifru na vytvorenie MAC hashovacej funkcie. Je možné naopak použiť MAC funkciu na blokovú šifru ? Skúste navrhnúť príslušný šifrovací systém a popíšte jeho bezpečnostné riziká.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. I want to bind the access to the database to the knowledge of the birth number without the date of birth (decadic four digits). Estimate the probability that in a class with 50 students there are at least two such students who have the same four-digit number (just estimate according to slide 5 of the lecture).

2. How can the birthday paradox be used to find the discrete logarithm? I know the value of y = gx mod p and want to compute x when I know p, a large prime number, and g, the generator of the corresponding cyclic group. (hints - compute gk mod p for a sufficient number of random numbers k and also compute y.g-r mod p for a sufficient number of numbers r ......). Describe the procedure in more detail and estimate its complexity.

3. Consider an authentication hash function Hn constructed using AES encryption with a known key K for the message M1, M2, ... Mn as follows: Hi = EK(Hi - 1 ⊕ Mi); H0 = 0. Show that this is not a good cryptographic hash function (it suffices for two-block messages - e.g., for a chosen A, find B such that H2(A,B) = H2(M1, M2) - for the known two-block message M1, M2).

4. The CBC-MAC hash (for IV=0) of the one-block message M is T. What will be the CBC-MAC hash of the two-block message M, M ⊕ T ?

\*. We have shown how a block cipher can be used to construct a MAC hash function. Conversely, is it possible to use a MAC function to make a block cipher ? Try to design an appropriate encryption scheme and describe its security risks.