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

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 4. 12. 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. Alica a Bob majú dohodnutý tajný kľúč, ktorý použijú na vzájomnú autentifikáciu použitím MAC funkcie takto:   
Bob vygeneruje výzvu (nonce) NB a pošle ju Alici  
 B→A : B, NBAlica pomocou tajného kľúča K hashuje MAC funkciou výzvu od Boba a pošle spolu so svojou výzvou NA   
 A→B : MACK(A, B, NB), NA Bob skontroluje správnosť kľúčovaného hashu (ktorý vie vyrobiť len ten, kto pozná kľúč K) a svoju identitu (dôkaz vedomosti kľúča K) preukáže hashovaním MAC funkciou Alicinej výzvy NA   
 B→A : MACK(B, A, NA) Alica skontroluje správnosť hashu, čím overí, že na druhej strane je niekto, kto tiež pozná K, teda Bob. Ukážte, že tento protokol nie je bezpečný (útočník sa môže autentifikovať využitím paralelných relácií s A aj B). Popíšte postup pri tomto útoku. Upravte protokol tak, aby sa tento útok nedal urobiť.

2. V miestnosti je päť ľudí. Práve jeden z nich je cudzí agent. Ostatní štyria poznajú také čísla, ktoré umožnia každej trojici vypočítať kľúč podľa Shamirovej schémy na zdieľanie tajomstva (s celočíselnými polynómami vo zvyškovej triede modulo 17). Cudzí agent si volí náhodné čísla. Pri preverovaní sa zistilo, že A pozná (1,2), B: (3,2), C: (5,10), D: (14,10) a E: (16,10). Kto je cudzí agent a aký je kľúč ? Skúste úlohu riešiť čo najefektívnejšie bez pomoci počítača – postup popíšte.

3. Navrhnite spôsob delenia tajomstva k odpáleniu hlavice v delostreleckom útvare s jedným generálom, tromi veliteľmi a desiatimi vojakmi, keď požadujem, aby hlavica mohla byť odpálená len v prítomnosti generála, alebo v prítomnosti aspoň dvoch veliteľov, alebo v prítomnosti veliteľa a aspoň troch vojakov, alebo v prítomnosti aspoň piatich vojakov. Ako by sa realizoval pomocou Shamirovej schémy? Vypočítajte len dôležité parametre - vhodné prvočíslo, stupeň polynómu, počet generovaných kľúčov a ich delenie.

\*. Chceme zvoliť heslo tak, aby odolalo jednomesačnému útoku rýchlosťou 10 miliónov pokusov za sekundu. Za predpokladu, že nepoužijeme žiadne slovníkové kombinácie, koľko znakov musí heslo minimálne obsahovať, pokiaľ vyberáme (náhodne)   
a) len malé písmená anglickej abecedy (26)   
b) alfanumerické reťazce s veľkými a malými písmenami a číslicami (62)   
c) všetky možné 7-bitové ASCII znaky (128) ?

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

1. Alice and Bob have agreed on a secret key, which they will use to authenticate each other using the MAC function as follows:   
Bob generates a challenge (nonce) NB and sends it to Alice  
 B→A : B, NB  
Alice uses the secret key K to hash Bob's challenge with the MAC function and sends it along with her challenge to NA   
 A→B : MACK(A, B, NB), NA   
Bob checks the correctness of the keyed hash (which only someone who knows the key K can produce) and proves his identity (proof of knowledge of the key K) by hashing the MAC function of Alice's challenge NA   
 B→A : MACK(B, A, NA)   
Alice checks the correctness of the hash, thus verifying that there is someone on the other side who also knows K, i.e. Bob. Show that this protocol is not secure (an attacker can authenticate by exploiting parallel sessions with both A and B). Describe the procedure for this attack. Modify the protocol so that this attack cannot be done.

2. There are five people in the room. Just one of them is a foreign agent. The other four know numbers such that each trio can compute a key according to Shamir's secret sharing scheme (with integer polynomials in the residue class modulo 17). The foreign agent has chosen random numbers. On inspection, it is found that A knows (1,2), B: (3,2), C: (5,10), D: (14,10), and E: (16,10). Who is the foreign agent and what is the key ? Try to solve the problem as efficiently as possible without the help of a computer - describe the procedure.

3. Suggest a method for dividing the secrecy required to fire a missile in an artillery formation with one general, three commanders, and ten soldiers, requiring that the missile can only be fired in the presence of the general, or in the presence of at least two commanders, or in the presence of a commander and at least three soldiers, or in the presence of at least five soldiers. How would it be implemented using Shamir's scheme? Calculate only the important parameters - the appropriate prime number, the degree of the polynomial, the number of keys to be generated, and their division.

\*. We want to choose a password to withstand a one-month attack at a rate of 10 million attempts per second. Assuming we do not use any dictionary combinations, how many characters must the password contain at a minimum if we are selecting (randomly)   
a) only the lower case letters of the English alphabet (26)   
b) alphanumeric strings with upper and lower case letters and numbers (62)   
c) all possible 7-bit ASCII characters (128) ?