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

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 11. 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. Analyzujte nasledujúci protokol, ktorým sa Alica a Bob chcú dohodnúť na krátkodobom kľúči K pomocou dlhodobého symetrického kľúča KAB :
 B→A : B, NB
 A→B : EKAB(NB, K)
 B→A : EK(NB)
Ukážte, či týmto protokolom dôjde k vzájomnej autentifikácii a či nemôže dôjsť k prezradeniu nového kľúča K. Skúste nájsť možný útok (odrazenie nadviazaním druhej relácie) a navrhnúť takú úpravu protokolu, aby bol tento útok vylúčený.

2. Alica a Bob sa chcú dohodnúť na tajnom kľúči Diffie-Hellmanovou výmenou. Dohodli sa na použití spoločného prvočísla p = 23 s generátorom g = 5. Ukážte, že 5 je generátorom multiplikatívnej grupy Z23\*. Aké je tajné číslo Alice, keď Bobovi pošle číslo 10 ? (vypočítajte hrubou silou). Aký bude nový tajný kľúč, keď Bob odpovie Alici číslom 4 ? (na to už hrubú silu netreba). Všetky výpočty urobte ručne (rýchlym modulárnym umocňovaním) !

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

1. Analyze the following protocol by which Alice and Bob want to agree on the short-term key K using the long-term symmetric key KAB :
 B→A : B, NB
 A→B : EKAB(NB, K)
 B→A : EK(NB)
Show whether this protocol will mutually authenticate and whether the new key K cannot be revealed. Try to find a possible attack (reflecting by establishing a second session) and propose a modification of the protocol such that this attack is avoided.

2. Alice and Bob want to agree on a secret Diffie-Hellman key exchange. They agree to use a common prime p = 23 with generator g = 5. Show that 5 is the generator of the multiplicative group Z23\*. What is Alice's secret number when she sends Bob the number 10 ? (calculate by brute force). What will be the new secret key when Bob responds to Alice with the number 4 ? (no more brute force needed for this). Do all calculations by hand (by fast modular exponentiation) !