4. samostatná práce z předmětu MKC-NSB
(Odevzdat do 23:59 dne **19.4.2022**)

Poznámky:

1. Odpověď na níže uvedené problémy koncipujte jako inženýři, tj. z Vaší odpovědi musí být jasný postup řešení a závěry musí být řádně a srozumitelně zdůvodněny.
2. Odpověď zpracujte ve vhodném textovém editoru (např. OpenOffice, LibreOffice, či Word). V použitém editoru využívejte funkce kreslení obrázků i matematických zápisů. Práci označte svým příjmením a odevzdejte ji ve formátu PDF. Pokud práce nebude splňovat uvedené požadavky, tak bude hodnocena 0 body.
3. Pokud Vám není něco jasné, tak se mi ozvěte na adresu: burda@vutbr.cz.

Problémy:

1. Protokol EAP (1,5 bodu)

Klient se vůči serveru autentizuje pomocí protokolu EAP. Jeho dokazovacím faktorem je klíč *K*, což je v kódu ASCII řetězec „Secret“. Znáte následující EAP zprávu:

01:13:00:0F:04:01:23:45:67:89:AB:CD:EF:01:23.

Určete, kdo je odesílatelem zprávy, jaký typ autentizace je použit a vysvětlete význam jednotlivých bajtů zprávy. Dále odvoďte bajtovou podobu EAP zprávy, která bude odezvou na zadanou EAP zprávu a význam bajtů této odezvy vysvětlete.

K překladu ASCII znaků klíče na bajty použijte ASCII tabulku z adresy:
https://cs.wikipedia.org/wiki/ASCII

K výpočtu heše použijte kalkulátor na adrese:
http://www.fileformat.info/tool/hash.htm

2. Protokol RADIUS (2,5 bodu)

Serveru byla z brány doručena následující zpráva protokolu RADIUS:

01:02:00:22:00:11:22:33:44:55:55:77:88:99:AA:BB:CC:DD:EE:FF:01:07:4A:6F:73:65:66:

02:07:F3:25:03:2A:BE.

Víme přitom, že k zabezpečení provozu mezi branou a serverem je používán klíč *K* = Secret.

U dané zprávy uveďte její typ a vysvětlete význam jednotlivých bajtů. Pokud se v ní vyskytuje přihlašovací jméno, tak je uveďte v textové podobě podle ASCII tabulky. Pokud se v ní bude nacházet zašifrované heslo, tak je dešifrujte a převeďte do textové podoby. Dále uveďte jaká bude odpověď serveru a význam jednotlivých bajtů této odpovědi vysvětlete. Předpokládejte přitom, že kontroly na straně serveru měly pozitivní výsledek.

K výpočtu hešů a ke konverzi bajtů na text použijte stejné odkazy jako v předchozím příkladu.