1. samostatná práce z předmětu MKC-NSB
(Odevzdat do 23:59 dne **21.2.2022**)

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@feec.vutbr.cz.

Něco k Vaší motivaci:

- Příklady všech samostatných prací se týkají problémů, které jsou pro daný obor důležité. Jejich vyřešením zmiňovaným problémům detailněji porozumíte a lépe si je zapamatujete. Protože problémy z příkladů máte zároveň i ve zkušebních otázkách, tak se řešením příkladu připravujete i ke zkoušce.
- Za vyřešení samostatné práce můžete obdržet až 4 body. Pro předmět s 5 kredity to odpovídá pracovnímu úsilí v trvání téměř 5 hodin. A těch 5 hodin chci na Vaší práci vidět!
- Obrázky kreslete zásadně v textovém editoru – pro budoucího inženýra musí být nakreslení jednoduchého obrázku v počítači bezproblémová rutina.
- Jako budoucí inženýři musíte být schopni o svých řešeních přesvědčit kolegy, šéfy a případně i zákazníky. Proto popis Vašich řešení musí být jasný a úplný.
- Dbejte také na odborné vyjadřování, formální úpravu (např. správné matematické symboly) i na pravopis. Tyto „drobnosti“ zvyšují Vaší hodnotu na trhu práce.
- Musíte se také naučit respektovat formální požadavky zadání. Pokud tedy máte za úkol práci odevzdat ve formátu PDF do termínu X a máte v ní uvést své příjmení, tak to udělejte. I to patří k profesionalitě.

Úvod:

- K některým výpočtům budete potřebovat provést operaci modulo (mod). Použijte k tomu vhodnou vědeckou kalkulačku, která touto operací disponuje. Ve Windows, či Linuxu stačí dedikovaná kalkulačka ve vědeckém režimu a pro mobily s Androidem je dobrá RealCalc.
- Připomínám, že operace XOR (⊕) je definována tak, že 0⊕0 = 1⊕1 = 0 a 0⊕1 = 1⊕0 = 1. Xorovat po bitech lze i bloky bitů o stejné délce. Například 0011⊕ 0101 = 0110.

Problémy:

1. Bloková šifra v režimu CBC.
Mějme zprávu Z = (13, 4, 9), kde jednotlivá čísla jsou bloky zprávy. Tuto zprávu zašifrujte v režimu CBC pro inicializační vektor IV = 6. Vypočítaný kryptogram pro kontrolu dešifrujte. Šifrování E a dešifrování D je dáno substitucemi podle tabulky 1. K provedení operací XOR si dekadická čísla převeďte na čtyřbitová čísla. Pro daný provozní režim nakreslete diagramy podle první přednáškové prezentace (snímek č. 21), přičemž v datových blocích schématu uveďte dekadicky i binárně hodnotu příslušného vstupu, či výstupu.

Tabulka 1: Šifrovací substituce y = E(x, K):

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
y	4	10	9	2	13	8	0	14	6	11	1	12	7	15	5	3

Pozn.: Při dešifrování je vstupem hodnota y a výstupem hodnota x.

2. Výpočet pečeti HMAC.

Mějme zprávu Z = (13, 4, 9), kde jednotlivá čísla jsou bloky zprávy. Pro tuto zprávu vypočítejte technikou HMAC pečeť P. Pečetící klíč K = 7, konstanta C_1 = 13 a C_2 = 8. K provedení operací XOR si dekadická čísla převeďte na čtyřbitová čísla. Hešovací funkce H je definována následovně:

$$h = \left(\sum_{i=1}^{t} a^i \cdot v_i\right) \bmod 17 \quad ,$$

kde hešovací konstanta a = 11, v_i je i-tý blok hešovaného vstupu a t počet bloků na vstupu. V prvém hešování tedy bude t = 4, protože první blok je výsledek xorování klíče a konstanty a další bloky jsou bloky zprávy. Ve druhém hešování bude t = 2. Pečetí P je výstup z druhého hešování, tj. $P = h_2$.

3. RSA podpis

Byla Vám doručena zpráva Z = (13, 4, 9), jejíž RSA podpis DS = 5. Ověřte, zda je tato zpráva autentická. Znáte veřejný ověřovací klíč udávaného autora VK = 3, jeho modulus n = 33 a víte, že byla použita hešovací funkce H ze 2. příkladu.