Cvičení 25.3.2024

Budeme pracovat se systémem Cryptool. Své odpovědi vložte do textového souboru (textového dokumentu), který uložíte ve formátu pdf. Odevzdejte jej do LMS do konce cvičení.

1. **DES vs AES a délka bloku.** Je dán otevřený text M AAAAAAAABBBBBBBBaaaaaaaabbbbbbbbAAAAAAAABBBBBBBB (jedná se o znaky ASCII, nikoliv hexadecimální reprezentaci). Jaký vliv má zvětšená velikost bloku algoritmu AES na vzory v šifrovém textu? Vysvětlete (a zkopírujte šifrové texty do dokumentu).
    a) Použijte DES v režimu (Encrypt/Decrypt → Symmetric (modern) →DES (ECB)).
    b) Použijte AES v ECB (Encrypt/Decrypt → Symmetric (modern) →Rijndael (AES)).
2. **DES ECB vs. DES CBC.** Vyřešte úlohu publikovanou zde https://samsclass.info/seminars/p6-124-image-ECB.html Jako řešení jsou potřeba oba šifrové texty (tj. oba zašifrované obrázky, zkopírujte je do dokumentu).
3. **DES – slabé klíče.** Proveďte šifrování textu z 1. úlohy pomocí DES ECB a DES CBC. Klíč bude 64 bitových jedniček (tj. FF FF FF FF FF FF FF FF). Výsledný šifrový text znovu zašifrujte stejným klíčem, který byl použit pro první šifrování. Co získáte (zkopírujte výsledek do dokumentu)? Existují nějaké jiné klíče, které by mohly mít stejný efekt (vyhledejte)? Jaké? Odpovězte.

Opakování ZŠ, SŠ, viz první kapitola skript Matematické základy kryptografických algoritmů (vsb.cz)

4. Jaké dělitele má číslo 24? Jaké dělitele má číslo 29? Jak určíte dělitelnost obecně?
5. Jsou čísla 120 a 49 soudělná či nesoudělná?
6. Nalezněte NSD(270, 36) a NSN(270, 36) pomocí kanonického rozkladu.