Cvičení 11.3.2024

1. Mějme zdroj informace generující dvě možné zprávy: „male“ nebo „female“ a nechť mají stejnou pravděpodobnost. Jaká je entropie zprávy z tohoto zdroje? (3. přednáška)

2. Co má vyšší entropii (neurčitost), hod (poctivou) kostkou, hod (poctivou) mincí nebo výběr jedné z barev v (poctivém) balíčku karet?

3. Mějme diskrétní náhodnou proměnnou X={a,b,c,d}, kde p(a)=1/3, p(b)=1/2, p(c)=1/12, p(d)=1/12.
    a) Jaká je její entropie?
    b) Pokud chceme vytvořit řetězec o 1000 symbolech skládající se ze symbolů {a, b,c,d}, jaké kódování (v bitech) bychom mohli zvolit a kolik bitů budeme potřebovat? Jakou roli bude hrát entropie?

4. Jaká je vzdálenost jednoznačnosti pro tyto šifry (pro angličtinu), pokud je rate r = 1.5:
    a) šifry Shift
    b) obecné jednoduché záměny
    c) transpozici (řádkovou), když je délka klíče 6 nebo 9

5. Někdy se šifrování spojuje také s kompresí zprávy. Jaké pořadí těchto operací byste zvolili a proč? Zvažte a zdůvodněte alespoň tři výhody takového spojení, případně nevýhody.

6. **Cryptool** – nainstalován na PC v učebně, ke stažení na webu nebo v LMS
7. Substituce: Zašifrujte a dešifrujte otevřený text M. pracujeme s anglickou abecedou bez mezery.
    a) Shift šifra
    b) Vigenèrova šifra s klíčem K = “KEY”.
8. Product Cipher. Zašifrujte M pomocí šifry ADFGVX se substitučním klíčem K_P = "MONDAY” a transpozičním klíčem (permutací) K_T = (3,4,2,1)

M = THIS TERMINAL IS NO MORE IT HAS CEASED TO BE ITS EXPIRED AND GONE TO MEET ITS MAKER THIS IS A LATE TERMINAL ITS A STIFF BEREFT OF LIFE IT RESTS IN PEACE IF YOU HADNT NAILED IT TO THE BENCH IT WOULD BE PUSHING UP THE DAISIES THIS IS AN XTERMINAL