

2016.01.13.

Vizsga
(Facebook csoport!)

- ① $p_1 = 0,8$
 $p_2 = 0,15$
 $p_3 = 0,05$

a) Elvi átlag kódlár → ENTROPIA!

$$H(x) = \sum_x p(x) \log_2 \left(\frac{1}{p_x} \right)$$

$$H(x) = 0,8 \log_2 \frac{1}{0,8} + 0,15 \log_2 \frac{1}{0,15} +$$

$$0,05 \log_2 \frac{1}{0,05} = \underline{\underline{0,8841}}$$

b) Átlagos kódlárhossz (SF) ?

$$\hat{L}_{SF} = \sum_x p(x) \cdot \left[\log_2 \frac{1}{p(x)} \right]$$

$$\hat{L}_{SF} = 0,8 \left[\log_2 \frac{1}{0,8} \right] + 0,15 \left[\log_2 \frac{1}{0,15} \right] +$$

$$+ 0,05 \left[\log_2 \frac{1}{0,05} \right] =$$

$$= 0,8 \cdot 1 + 0,15 \cdot 3 + 0,05 \cdot 5 = 1,5$$

⑤ GF(8) RS

$$g(x) = x^5 + y^4 x + y^3$$

a) Häufigkeit t der Faktoren?

$$t = \left\lfloor \frac{n-k}{2} \right\rfloor$$

GF(q)

$$q = n-1 \rightarrow n = 7$$

$$\deg(g(x)) = n-k$$

$$k = 7 - k$$

$$5 = k$$

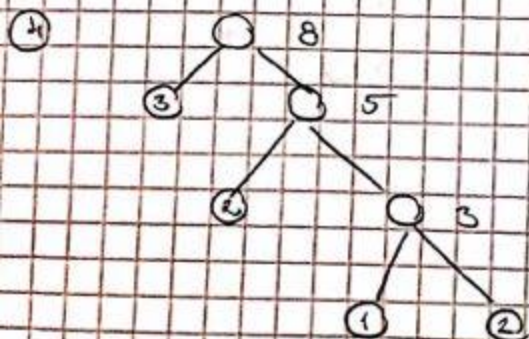
C(7, 5)

$$t = \left\lfloor \frac{7-5}{2} \right\rfloor = \underline{\underline{1}}$$

b) Partialschrittweite polinom faktorisierte:

$$\deg(r(x)) = k$$

$$\underline{\underline{k=5}}$$



(Ergebnis alle Faktoren
a. Hergewinnung)

⑤ RSA

$$p_1 = 13$$

$$p_2 = 19$$

$$\phi(m) = ?$$

$$\phi(m) = \prod_1^n (p_n - 1)$$

$$\phi(m) = (13 - 1)(19 - 1) = 12 \cdot 18 = \underline{\underline{216}}$$