(1) $m'(x) = 1+x^3+x^4$ $p(x) = 1+x+x^3$

$m(x) = r(x) + x^3\cdot m'(x)$ $(x^3\cdot m'(x)) : p(x) = q(x)\cdot p(x) + r(x)$

$(x^3+x^6+x^7):(1+x+x^3) = x^4+x^3+x^2+1$

$x^4+x^5+x^7$

$x^3+x^4+x^5+x^6$

$x^3+x^4+x^6$

x^5

$x^2+x^3+x^5$

$1+x+x^3$

$1+x+x^2$

$m(x) = r(x) + q(x)\cdot p(x) + r(x)$

3 27-8:01

(2) $m_1 = 10000$

$m_2 = 01000$

$m_3 = 00100$

$m_4 = 00010$

$m_5 = 00001$

$x^5 : 1+x+x^3 = x^2+1$

$x^2+x^3+x^5$

$1+x+x^3$

$1+x+x^2 = r(x)$

$m(x) = 1+x+x^2+x^5$

$G = \begin{pmatrix} P \\ I_5 \end{pmatrix}$ $H = (I_3\ P)$

$H\cdot G = P+P = 0$

$m \mapsto G\cdot m \mapsto H(G\cdot m)$

3 27-8:12

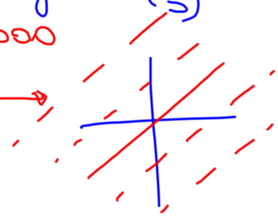
(3) $\begin{pmatrix} 1&0&0&1&0&1&1&1 \\ 0&1&0&1&1&1&0&0 \\ 0&0&1&0&1&1&1&0 \end{pmatrix} \cdot \begin{pmatrix}1\\0\\0\\0\\1\\1\\1\\1\end{pmatrix} = \begin{pmatrix}0\\0\\1\end{pmatrix}$

(I_3, P)

2^5 kódových slov má syndrom $\begin{pmatrix}0\\0\\0\end{pmatrix}$

hledaný vektor 00100000 je vedoucí reprezentant

=> původní zpráva je 10101111



3 27-8:19

RSA $N = p\cdot q$ p, q prvočísla

$(e, \varphi(N)) = 1$, $d = e^{-1} \bmod \varphi(N)$

$M \mapsto M^e \bmod N$

$p = 11$, $q = 13$, $e = 17$, $N = 11\cdot 13 = 143$

$\varphi(143) = \varphi(11)\cdot\varphi(13) = 10\cdot 12 = 120$

$(17,120) = 1 \Rightarrow 1 = a\cdot 17 + b\cdot 120$

3 27-8:30

$120 = 7\cdot 17 + 1$

$1 = 120 - 7\cdot 17$

$\Rightarrow d = -7 \bmod 120$
$= 113 \bmod 120$

$3^{17} = (3^8)^2\cdot 3 = ((3^4)^2)^2\cdot 3 = \dots = 9$

$3 \quad 3^2\cdot 3^5\cdot 3^5\cdot 3^5 \bmod 9$

$\mathbb{Z}_{\varphi(N)}$

3 27-8:42

$x = 10$, $g = 11$, $G = \mathbb{Z}_{41}$

$11^{10} \equiv 9 \bmod 41$

veřejný $(\mathbb{Z}_{41}, 11, 9)$ (h)

$(22, 6)$ $11^y \equiv 22 \bmod 41$

$z\cdot 9^y \equiv 6 \bmod 41$

$m = s_2 / s_1^x \equiv 6/22^{10} \bmod 41$

$484 : 41 = -8 \bmod 41$

3 27-9:05