Reed-Solomon-Code

Joshua Bär und Michael Steiner

OST Ostschweizer Fachhochschule

26.04.2021

Reed-Solomon-Code:

- Für Übertragung von Daten

Reed-Solomon-Code:

- Für Übertragung von Daten
- Ermöglicht Korrektur von Übertragungsfehler

Reed-Solomon-Code:

- Für Übertragung von Daten
- Ermöglicht Korrektur von Übertragungsfehler
- Wird verwendet in: CD, QR-Codes, Voyager-Sonde, etc.

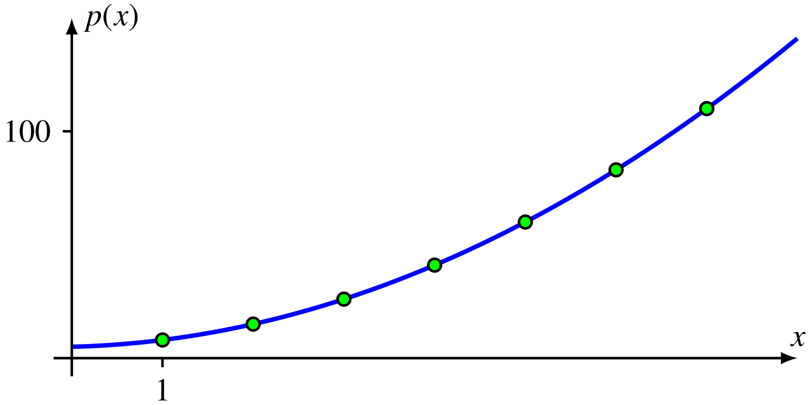
- Beispiel $2, 1, 5$ versenden und auf 2 Fehler absichern

Beispiel

Übertragen von $f_2 = 2$, $f_1 = 1$, $f_0 = 5$ als $p(w) = 2w^2 + 1w + 5$.
Versende $(p(1), p(2), \ldots, p(7))$

Beispiel

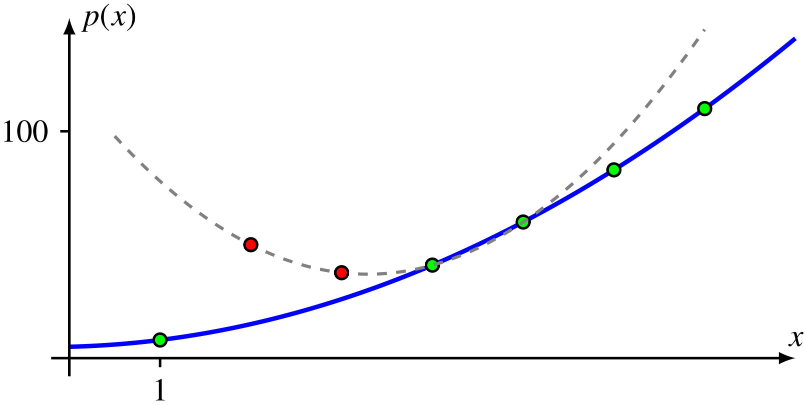
Übertragen von $f_2 = 2$, $f_1 = 1$, $f_0 = 5$ als $p(w) = 2w^2 + 1w + 5$.
Versende $(p(1), p(2), \ldots, p(7)) = (8, 15, 26, 41, 60, 83, 110)$



Beispiel

Übertragen von $f_2 = 2$, $f_1 = 1$, $f_0 = 5$ als $p(w) = 2w^2 + 1w + 5$.

Versende $(p(1), p(2), \dots, p(7)) = (8, 50, 37, 41, 60, 83, 110)$



7 Zahlen versenden, um 3 Zahlen gegen 2 Fehlern abzusichern.

Parameter

“Nutzlast”	Fehler	Versenden
3	2	7 Werte eines Polynoms vom Grad 2
4	2	8 Werte eines Polynoms vom Grad 3

Parameter

“Nutzlast”	Fehler	Versenden
3	2	7 Werte eines Polynoms vom Grad 2
4	2	8 Werte eines Polynoms vom Grad 3
3	3	

Parameter

“Nutzlast”	Fehler	Versenden
3	2	7 Werte eines Polynoms vom Grad 2
4	2	8 Werte eines Polynoms vom Grad 3
3	3	9 Werte eines Polynoms vom Grad 2

Parameter

“Nutzlast”	Fehler	Versenden
3	2	7 Werte eines Polynoms vom Grad 2
4	2	8 Werte eines Polynoms vom Grad 3
3	3	9 Werte eines Polynoms vom Grad 2
k	t	$k+2t$ Werte eines Polynoms vom Grad $k-1$

Ausserdem können bis zu $2t$ Fehler erkannt werden!

Einführung

Polynom Ansatz

Diskrete Fourier Transformation

Reed-Solomon in Endlichen Körpern

Codierung eines Beispiels

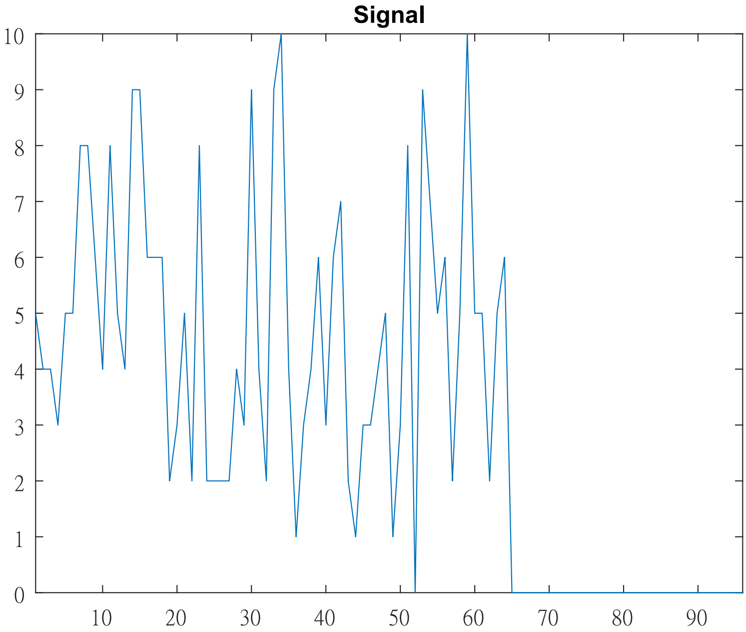
Decodierung ohne Fehler

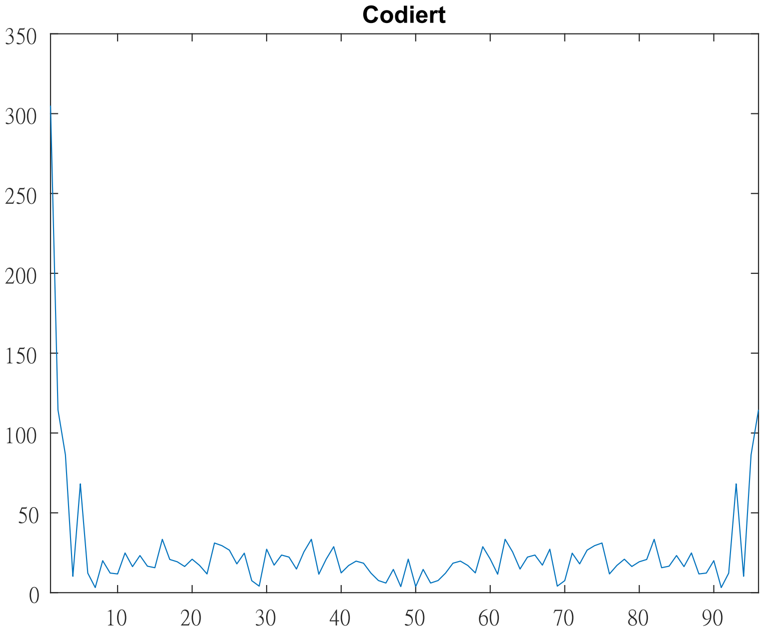
Decodierung mit Fehler

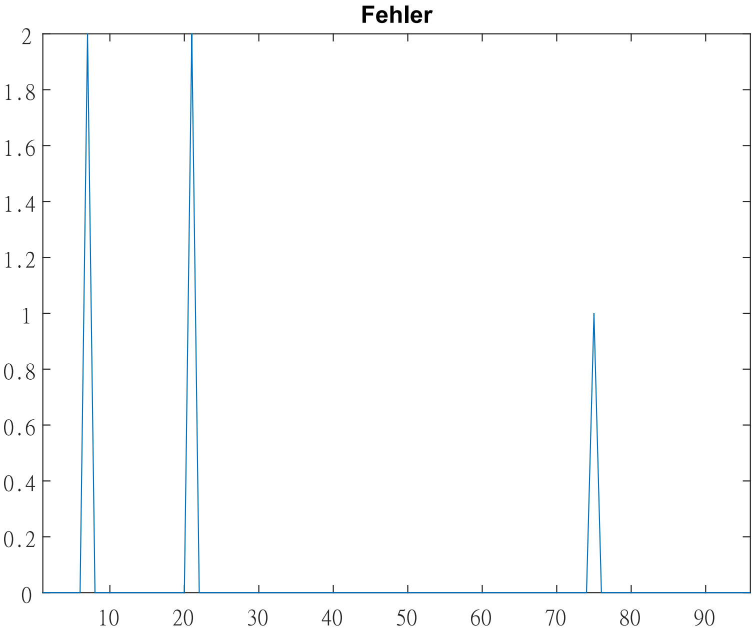
Nachricht Rekonstruieren

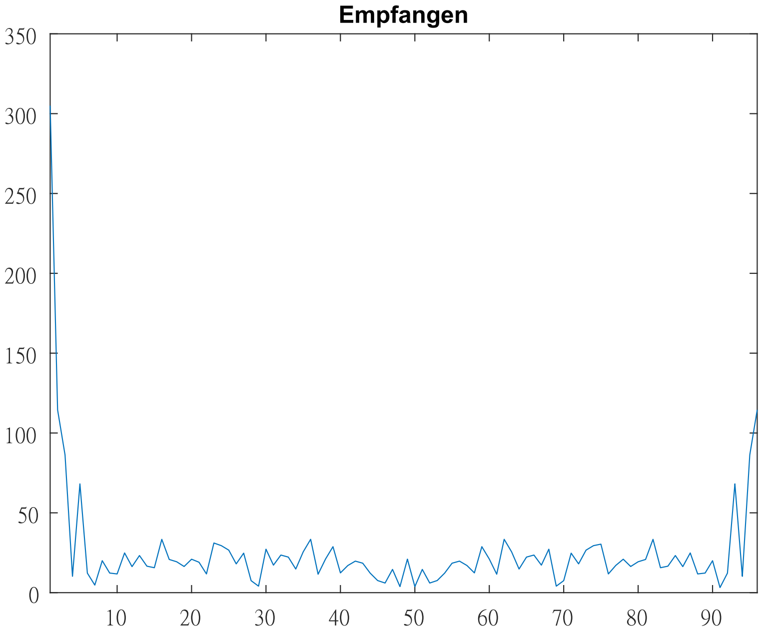
Idee

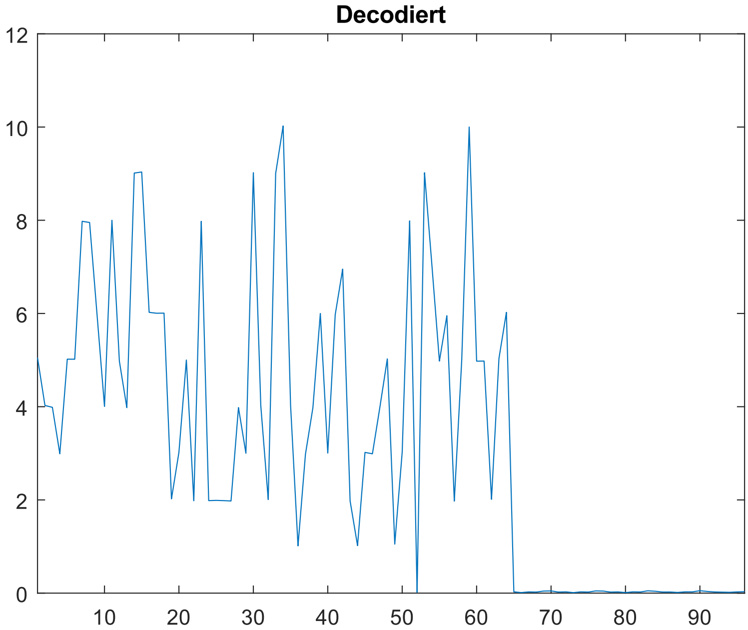
- Fourier-transformieren
- Übertragung
- Rücktransformieren

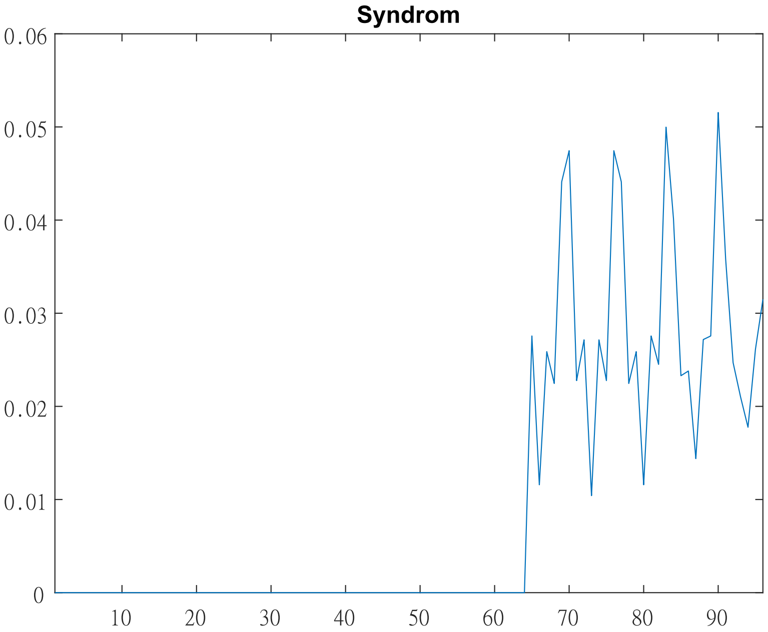

Signal
0
1
2
3
4
5
6
7
8
9
10
10
20
30
40
50
60
70
80
90

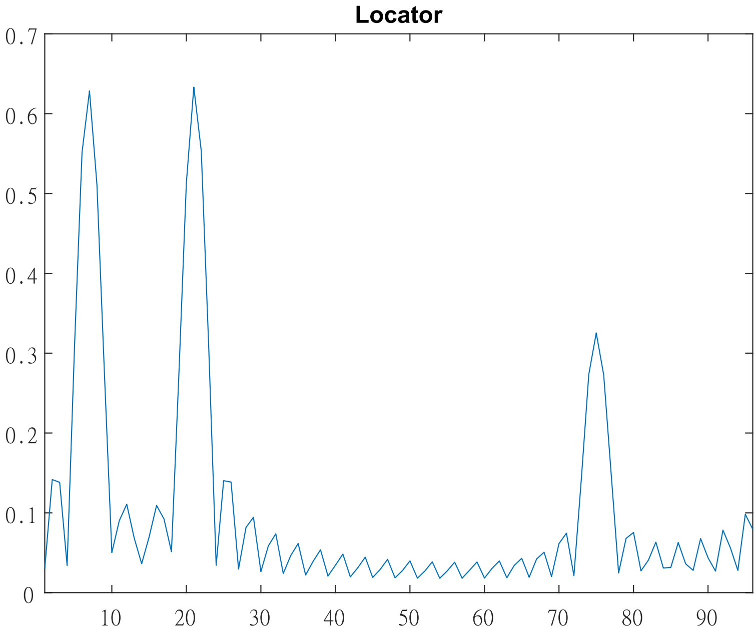

Codiert
350
300
250
200
150
100
50
0
10
20
30
40
50
60
70
80
90


Fehler
2
1.8
1.6
1.4
1.2
1
0.8
0.6
0.4
0.2
0
10
20
30
40
50
60
70
80
90


Empfangen
350
300
250
200
150
100
50
0
10
20
30
40
50
60
70
80
90


Decodiert
0
2
4
6
8
10
12
10
20
30
40
50
60
70
80
90


Syndrom
0.06
0.05
0.04
0.03
0.02
0.01
0
10
20
30
40
50
60
70
80
90


Locator
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
10
20
30
40
50
60
70
80
90

Diskrete Fourier Transformation

- Diskrete Fourier-Transformation gegeben durch:

$$\hat{c}_k = \frac{1}{N} \sum_{n=0}^{N-1} f_n \cdot e^{-\frac{2\pi j}{N} \cdot kn}$$

Diskrete Fourier Transformation

- Diskrete Fourier-Transformation gegeben durch:

$$\hat{c}_k = \frac{1}{N} \sum_{n=0}^{N-1} f_n \cdot e^{-\frac{2\pi j}{N} \cdot kn}$$

- Ersetzte

$$w = e^{-\frac{2\pi j}{N} k}$$

Diskrete Fourier Transformation

- Diskrete Fourier-Transformation gegeben durch:

$$\hat{c}_k = \frac{1}{N} \sum_{n=0}^{N-1} f_n \cdot e^{-\frac{2\pi j}{N} \cdot kn}$$

- Ersetzte

$$w = e^{-\frac{2\pi j}{N} k}$$

- Wenn N konstant:

$$\hat{c}_k = \frac{1}{N}(f_0 w^0 + f_1 w^1 + f_2 w^2 + \cdots + f_{N-1} w^N)$$

Diskrete Fourier Transformation

$$
\begin{pmatrix} \hat{c}_1 \\ \hat{c}_2 \\ \hat{c}_3 \\ \vdots \\ \hat{c}_n \end{pmatrix} = \frac{1}{N} \begin{pmatrix} w^0 & w^0 & w^0 & \dots & w^0 \\ w^0 & w^1 & w^2 & \dots & w^{N-1} \\ w^0 & w^2 & w^4 & \dots & w^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ w^0 & w^{1(N-1)} & w^{2(N-1)} & \dots & w^{(N-1)(N-1)} \end{pmatrix} \begin{pmatrix} f_0 \\ f_1 \\ f_2 \\ \vdots \\ 0 \end{pmatrix}
$$

Probleme und Fragen

Wie wird der Fehler lokalisiert?

Probleme und Fragen

Wie wird der Fehler lokalisiert?
Indem in einem endlichen Körper gerechnet wird.

Reed-Solomon in Endlichen Körpern

- Warum endliche Körper?
  konkrete Zahlen $\rightarrow$ keine Rundungsfehler
  digitale Fehlerkorrektur
  bessere Laufzeit
- Nachricht $=$ Nutzdaten $+$ Fehlerkorrekturteil
- aus Fehlerkorrekturteil die Fehlerstellen finden
  $\Rightarrow$ gesucht ist ein Lokatorpolynom

Definition eines Beispiels

- endlicher Körper $q = 11$
  ist eine Primzahl
  beinhaltet die Zahlen $\mathbb{F}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
- Nachrichtenblock $=$ Nutzlast $+$ Fehlerkorrekturstellen
  $n = q - 1 = 10$ Zahlen
- Max. Fehler $z = 2$
  maximale Anzahl von Fehler, die wir noch korrigieren können
- Nutzlast $k = n - 2t = 6$ Zahlen
  Fehlerkorrkturstellen $2t = 4$ Zahlen
  Nachricht $m = [0, 0, 0, 0, 4, 7, 2, 5, 8, 1]$
  als Polynom $m(X) = 4X^5 + 7X^4 + 2X^3 + 5X^2 + 8X + 1$

Codierung

- Ansatz aus den komplexen Zahlen mit der diskreten Fouriertransformation
- Eulersche Zahl e existiert nicht in $\mathbb{F}_{11}$
- Wir suchen a so, dass a^i den gesamten Zahlenbereich von $\mathbb{F}_{11}$ abdecken
  $\mathbb{Z}_{11} \setminus \{0\} = \{a^0, a^1, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9\}$
- Wir wählen $a = 8$
  $\mathbb{Z}_{11} \setminus \{0\} = \{1, 8, 9, 6, 4, 10, 3, 2, 5, 7\}$
  8 ist eine primitive Einheitswurzel
- $m(8^0) = 4 \cdot 1 + 7 \cdot 1 + 2 \cdot 1 + 5 \cdot 1 + 8 \cdot 1 + 1 = 5$
  $\Rightarrow$ können wir auch als Matrix schreiben

Codierung

- Übertragungsvektor v
- $v = A \cdot m$

$$v = \begin{pmatrix} 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 \\ 8^0 & 8^1 & 8^2 & 8^3 & 8^4 & 8^5 & 8^6 & 8^7 & 8^8 & 8^9 \\ 8^0 & 8^2 & 8^4 & 8^6 & 8^8 & 8^{10} & 8^{12} & 8^{14} & 8^{16} & 8^{18} \\ 8^0 & 8^3 & 8^6 & 8^9 & 8^{12} & 8^{15} & 8^{18} & 8^{21} & 8^{24} & 8^{27} \\ 8^0 & 8^4 & 8^8 & 8^{12} & 8^{16} & 8^{20} & 8^{24} & 8^{28} & 8^{32} & 8^{36} \\ 8^0 & 8^5 & 8^{10} & 8^{15} & 8^{20} & 8^{25} & 8^{30} & 8^{35} & 8^{40} & 8^{45} \\ 8^0 & 8^6 & 8^{12} & 8^{18} & 8^{24} & 8^{30} & 8^{36} & 8^{42} & 8^{48} & 8^{54} \\ 8^0 & 8^7 & 8^{14} & 8^{21} & 8^{28} & 8^{35} & 8^{42} & 8^{49} & 8^{56} & 8^{63} \\ 8^0 & 8^8 & 8^{16} & 8^{24} & 8^{32} & 8^{40} & 8^{48} & 8^{56} & 8^{64} & 8^{72} \\ 8^0 & 8^9 & 8^{18} & 8^{27} & 8^{36} & 8^{45} & 8^{54} & 8^{63} & 8^{72} & 8^{81} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 8 \\ 5 \\ 2 \\ 7 \\ 4 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

- $v = [5, 3, 6, 5, 2, 10, 2, 7, 10, 4]$

Decodierung ohne Fehler

- Der Empfänger erhält den unveränderten Vektor $v = [5, 3, 6, 5, 2, 10, 2, 7, 10, 4]$
- Wir suchen die Inverse der Matrix A

Inverse der Fouriertransformation

$$F(\omega) = \int_{-\infty}^{\infty} f(t)\mathrm{e}^{-j\omega t} dt$$

$$\mathfrak{F}^{-1}(F(\omega)) = f(t) = \frac{1}{2\pi}\int_{-\infty}^{\infty} F(\omega)\mathrm{e}^{j\omega t} d\omega$$

Inverse von a

$$8^1 \Rightarrow 8^{-1}$$

Inverse finden wir über den Eulkidischen Algorithmus

Der Euklidische Algorithmus

Recap aus der Vorlesung:
Gegeben $a \in \mathbb{F}_p$, finde $b = a^{-1} \in \mathbb{F}_p$

$$\begin{aligned} ab &\equiv 1 \mod p \\ ab &= 1 + np \\ ab - np &= 1 \end{aligned}$$

$$\begin{aligned} \operatorname{ggT}(a, p) &= 1 \\ sa + tp &= 1 \\ b &= s \\ n &= -t \end{aligned}$$

k	a_i	b_i	q_i	c_i	d_i
				1	0
0	8	11	0	0	1
1	11	8	1	1	0
2	8	3	2	-1	1
3	3	2	1	3	-2
4	2	1	2	-4	3
5	1	0		11	-8

$$\begin{aligned} -4 \cdot 8 + 3 \cdot 11 &= 1 \\ 7 \cdot 8 + 3 \cdot 11 &= 1 \\ 8^{-1} &= 7 \end{aligned}$$

Der Euklidische Algorithmus

Recap aus der Vorlesung:
Gegeben $a \in \mathbb{F}_p$, finde $b = a^{-1} \in \mathbb{F}_p$

$$\begin{aligned} ab &\equiv 1 \mod p \\ ab &= 1 + np \\ ab - np &= 1 \end{aligned}$$

$$\begin{aligned} \operatorname{ggT}(a, p) &= 1 \\ sa + tp &= 1 \\ b &= s \\ n &= -t \end{aligned}$$

k	a_i	b_i	q_i	c_i	d_i
				1	0
0	8	11	0	0	1
1	11	8	1	1	0
2	8	3	2	−1	1
3	3	2	1	3	−2
4	2	1	2	−4	3
5	1	0		11	−8

$$\begin{aligned} -4 \cdot 8 + 3 \cdot 11 &= 1 \\ 7 \cdot 8 + 3 \cdot 11 &= 1 \\ 8^{-1} &= 7 \end{aligned}$$

Der Euklidische Algorithmus

Recap aus der Vorlesung:
Gegeben $a \in \mathbb{F}_p$, finde $b = a^{-1} \in \mathbb{F}_p$

$$\begin{aligned} ab &\equiv 1 \mod p \\ ab &= 1 + np \\ ab - np &= 1 \end{aligned}$$

$$\begin{aligned} \operatorname{ggT}(a, p) &= 1 \\ sa + tp &= 1 \\ b &= s \\ n &= -t \end{aligned}$$

k	a_i	b_i	q_i	c_i	d_i
				1	0
0	8	11	0	0	1
1	11	8	1	1	0
2	8	3	2	-1	1
3	3	2	1	3	-2
4	2	1	2	-4	3
5	1	0		11	-8

$$\begin{aligned} -4 \cdot 8 + 3 \cdot 11 &= 1 \\ 7 \cdot 8 + 3 \cdot 11 &= 1 \\ 8^{-1} &= 7 \end{aligned}$$

Decodierung mit Inverser Matrix

- $v = [5, 3, 6, 5, 2, 10, 2, 7, 10, 4]$
- $m = 1/10 \cdot A^{-1} \cdot v$
- $m = 10 \cdot A^{-1} \cdot v$

$$m = \begin{pmatrix} 7^0 & 7^0 & 7^0 & 7^0 & 7^0 & 7^0 & 7^0 & 7^0 & 7^0 & 7^0 \\ 7^0 & 7^1 & 7^2 & 7^3 & 7^4 & 7^5 & 7^6 & 7^7 & 7^8 & 7^9 \\ 7^0 & 7^2 & 7^4 & 7^6 & 7^8 & 7^{10} & 7^{12} & 7^{14} & 7^{16} & 7^{18} \\ 7^0 & 7^3 & 7^6 & 7^9 & 7^{12} & 7^{15} & 7^{18} & 7^{21} & 7^{24} & 7^{27} \\ 7^0 & 7^4 & 7^8 & 7^{12} & 7^{16} & 7^{20} & 7^{24} & 7^{28} & 7^{32} & 7^{36} \\ 7^0 & 7^5 & 7^{10} & 7^{15} & 7^{20} & 7^{25} & 7^{30} & 7^{35} & 7^{40} & 7^{45} \\ 7^0 & 7^6 & 7^{12} & 7^{18} & 7^{24} & 7^{30} & 7^{36} & 7^{42} & 7^{48} & 7^{54} \\ 7^0 & 7^7 & 7^{14} & 7^{21} & 7^{28} & 7^{35} & 7^{42} & 7^{49} & 7^{56} & 7^{63} \\ 7^0 & 7^8 & 7^{16} & 7^{24} & 7^{32} & 7^{40} & 7^{48} & 7^{56} & 7^{64} & 7^{72} \\ 7^0 & 7^9 & 7^{18} & 7^{27} & 7^{36} & 7^{45} & 7^{54} & 7^{63} & 7^{72} & 7^{81} \end{pmatrix} \cdot \begin{pmatrix} 5 \\ 3 \\ 6 \\ 5 \\ 2 \\ 10 \\ 2 \\ 7 \\ 10 \\ 4 \end{pmatrix}$$

- $m = [0, 0, 0, 0, 4, 7, 2, 5, 8, 1]$

Decodierung mit Fehler - Ansatz

- Gesendet: $v = [5, 3, 6, 5, 2, 10, 2, 7, 10, 4]$
- Empfangen: $w = [5, 3, 6, 8, 2, 10, 2, 7, 1, 4]$
- Rücktransformation: $r = [\underbrace{5, 7, 4, 10,}_{\textit{Fehlerinfo}} 5, 4, 5, 7, 6, 7]$

Wie finden wir die Fehler?

- $m(X) = 4X^5 + 7X^4 + 2X^3 + 5X^2 + 8X + 1$
- $r(X) = 5X^9 + 7X^8 + 4X^7 + 10X^6 + 5X^5 + 4X^4 + 5X^3 + 7X^2 + 6X + 7$
- $e(X) = r(X) - m(X)$

i	0	1	2	3	4	5	6	7	8	9
$r(a^i)$	5	3	6	8	2	10	2	7	1	4
$m(a^i)$	5	3	6	5	2	10	2	7	10	4
$e(a^i)$	0	0	0	3	0	0	0	0	2	0

- Alle Stellen, die nicht Null sind, sind Fehler

Nullstellen des Fehlerpolynoms finden

- Satz von Fermat: $f(X) = X^{q-1} - 1 = 0$
- $f(X) = X^{10} - 1 = 0 \qquad \text{für } X \in \{1,2,3,4,5,6,7,8,9,10\}$
- $f(X) = (X-a^0)(X-a^1)(X-a^2)(X-a^3)(X-a^4)(X-a^5)(X-a^6)\cdot (X-a^7)(X-a^8)(X-a^9)$
- $e(X) = (X-a^0)(X-a^1)(X-a^2) \qquad (X-a^4)(X-a^5)(X-a^6)\cdot (X-a^7) \qquad (X-a^9)\cdot p(x)$
- ggT gibt uns eine Liste der Nullstellen, an denen es keine Fehler gegeben hat

$$\mathrm{ggT}(f(X), e(X)) = (X-a^0)(X-a^1)(X-a^2) \qquad (X-a^4)(X-a^5)(X-a^6)\cdot (X-a^7) \qquad (X-a^9)$$

Nullstellen des Fehlerpolynoms finden

- Satz von Fermat: $f(X) = X^{q-1} - 1 = 0$
- $f(X) = X^{10} - 1 = 0 \qquad$ für $X = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10]$
- $$f(X) = (X - a^0)(X - a^1)(X - a^2)(X - a^3)(X - a^4)(X - a^5)(X - a^6)\cdot (X - a^7)(X - a^8)(X - a^9)$$
- $$e(X) = (X - a^0)(X - a^1)(X - a^2) \qquad (X - a^4)(X - a^5)(X - a^6)\cdot (X - a^7) \qquad (X - a^9) \cdot p(x)$$
- kgV gibt uns eine Liste von aller Nullstellen, die wir in e und d zerlegen können

  $$\text{kgV}(f(X), e(X)) = (X - a^0)(X - a^1)(X - a^2)(X - a^3)(X - a^4)(X - a^5)(X - a^6)\cdot (X - a^7)(X - a^8)(X - a^9) \cdot q(X)$$
  $$= d(X) \cdot e(X)$$
- Lokatorpolynom $d(X) = (X - a^3)(X - a^8)$

Kennen wir $e(X)$?

- $e(X)$ ist unbekannt auf der Empfängerseite
- $e(X) = r(X) - m(X) \qquad \rightarrow \qquad m(X)$ ist unbekannt?
- m ist nicht gänzlich unbekannt: $m = [0, 0, 0, 0, ?, ?, ?, ?, ?, ?]$
  In den bekannten Stellen liegt auch die Information, wo es Fehler gegeben hat
- Daraus folgt $e(X) = 5X^9 + 7X^8 + 4X^7 + 10X^6 + p(X)$
- $f(X) = X^{10} - 1 = X^{10} + 10$
- Jetzt können wir den ggT von $f(X)$ und $e(X)$ berechnen

Der Euklidische Algorithmus (nochmal)

$\operatorname{ggT}(f(X), e(X))$ hat den Grad 8

$$
\begin{array}{r}
X^{10} \qquad\qquad\qquad\qquad\qquad + \;\; 10 \\
\underline{X^{10} + 8X^9 + 3X^8 + 2X^7 + p(X)} \\
3X^9 + 8X^8 + 9X^7 + p(X) \\
\underline{3X^9 + 2X^8 + 9X^7 + p(X)} \\
6X^8 + 0X^7 + p(X)
\end{array}
\quad : 5X^9 + 7X^8 + 4X^7 + 10X^6 + p(X) = 9X + 5
$$

$$
\begin{array}{r}
5X^9 + 7X^8 + \; 4X^7 + 10X^6 + p(X) \\
\underline{5X^9 + 0X^8 + p(X)} \\
7X^8 + p(X)
\end{array}
\quad : 6X^8 + 0X^7 \qquad = 10X + 3
$$

$\operatorname{ggT}(f(X), e(X)) = 6X^8$

kgV durch den erweiterten Euklidischen Algorithmus bestimmen

Der Erweiterte Euklidische Algorithmus

k	q_i	e_i	f_i
		0	1
0	$9X+5$	1	0
1	$10X+3$	$9X+5$	1
2		$2X^2+0X+5$	$10X+3$

Somit erhalten wir den Faktor $d(X) = 2X^2 + 5$

Faktorisiert erhalten wir $d(X) = 2(X-5)(X-6)$

Lokatorpolynom $d(X) = (X-a^i)(X-a^i)$

$$a^i = 5 \quad \Rightarrow \quad i = 3$$
$$a^i = 6 \quad \Rightarrow \quad i = 8$$

$$d(X) = (X-a^3)(X-a^8)$$

Der Erweiterte Euklidische Algorithmus

k	q_i	e_i	f_i
		0	1
0	$9X+5$	1	0
1	$10X+3$	$9X+5$	1
2		$2X^2+0X+5$	$10X+3$

Somit erhalten wir den Faktor $d(X) = 2X^2 + 5$

Faktorisiert erhalten wir $d(X) = 2(X-5)(X-6)$

Lokatorpolynom $d(X) = (X-a^i)(X-a^i)$

$$a^i = 5 \quad \Rightarrow \quad i = 3$$
$$a^i = 6 \quad \Rightarrow \quad i = 8$$

$$d(X) = (X-a^3)(X-a^8)$$

Rekonstruktion der Nachricht

- $w = [5, 3, 6, 8, 2, 10, 2, 7, 1, 4]$
- $d(X) = (X - a^3)(X - a^8)$

$$
\begin{pmatrix} a^0 \\ a^1 \\ a^2 \\ a^3 \\ a^4 \\ a^5 \\ a^6 \\ a^7 \\ a^8 \\ a^9 \end{pmatrix}
\begin{pmatrix} 5 \\ 3 \\ 6 \\ 8 \\ 2 \\ 10 \\ 2 \\ 7 \\ 1 \\ 4 \end{pmatrix}
=
\begin{pmatrix}
8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 \\
8^0 & 8^1 & 8^2 & 8^3 & 8^4 & 8^5 & 8^6 & 8^7 & 8^8 & 8^9 \\
8^0 & 8^2 & 8^4 & 8^6 & 8^8 & 8^{10} & 8^{12} & 8^{14} & 8^{16} & 8^{18} \\
8^0 & 8^3 & 8^6 & 8^9 & 8^{12} & 8^{15} & 8^{18} & 8^{21} & 8^{24} & 8^{27} \\
8^0 & 8^4 & 8^8 & 8^{12} & 8^{16} & 8^{20} & 8^{24} & 8^{28} & 8^{32} & 8^{36} \\
8^0 & 8^5 & 8^{10} & 8^{15} & 8^{20} & 8^{25} & 8^{30} & 8^{35} & 8^{40} & 8^{45} \\
8^0 & 8^6 & 8^{12} & 8^{18} & 8^{24} & 8^{30} & 8^{36} & 8^{42} & 8^{48} & 8^{54} \\
8^0 & 8^7 & 8^{14} & 8^{21} & 8^{28} & 8^{35} & 8^{42} & 8^{49} & 8^{56} & 8^{63} \\
8^0 & 8^8 & 8^{16} & 8^{24} & 8^{32} & 8^{40} & 8^{48} & 8^{56} & 8^{64} & 8^{72} \\
8^0 & 8^9 & 8^{18} & 8^{27} & 8^{36} & 8^{45} & 8^{54} & 8^{63} & 8^{72} & 8^{81}
\end{pmatrix}
\cdot
\begin{pmatrix} m_0 \\ m_1 \\ m_2 \\ m_3 \\ m_4 \\ m_5 \\ m_6 \\ m_7 \\ m_8 \\ m_9 \end{pmatrix}
$$

- Fehlerstellen entfernen

Rekonstruktion der Nachricht

- $w = [5, 3, 6, 8, 2, 10, 2, 7, 1, 4]$
- $d(X) = (X - a^3)(X - a^8)$

$$\begin{pmatrix} a^0 \\ a^1 \\ a^2 \\ a^3 \\ a^4 \\ a^5 \\ a^6 \\ a^7 \\ a^8 \\ a^9 \end{pmatrix} \begin{pmatrix} 5 \\ 3 \\ 6 \\ 8 \\ 2 \\ 10 \\ 2 \\ 7 \\ 1 \\ 4 \end{pmatrix} = \begin{pmatrix} 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 \\ 8^0 & 8^1 & 8^2 & 8^3 & 8^4 & 8^5 & 8^6 & 8^7 & 8^8 & 8^9 \\ 8^0 & 8^2 & 8^4 & 8^6 & 8^8 & 8^{10} & 8^{12} & 8^{14} & 8^{16} & 8^{18} \\ 8^0 & 8^3 & 8^6 & 8^9 & 8^{12} & 8^{15} & 8^{18} & 8^{21} & 8^{24} & 8^{27} \\ 8^0 & 8^4 & 8^8 & 8^{12} & 8^{16} & 8^{20} & 8^{24} & 8^{28} & 8^{32} & 8^{36} \\ 8^0 & 8^5 & 8^{10} & 8^{15} & 8^{20} & 8^{25} & 8^{30} & 8^{35} & 8^{40} & 8^{45} \\ 8^0 & 8^6 & 8^{12} & 8^{18} & 8^{24} & 8^{30} & 8^{36} & 8^{42} & 8^{48} & 8^{54} \\ 8^0 & 8^7 & 8^{14} & 8^{21} & 8^{28} & 8^{35} & 8^{42} & 8^{49} & 8^{56} & 8^{63} \\ 8^0 & 8^8 & 8^{16} & 8^{24} & 8^{32} & 8^{40} & 8^{48} & 8^{56} & 8^{64} & 8^{72} \\ 8^0 & 8^9 & 8^{18} & 8^{27} & 8^{36} & 8^{45} & 8^{54} & 8^{63} & 8^{72} & 8^{81} \end{pmatrix} \cdot \begin{pmatrix} m_0 \\ m_1 \\ m_2 \\ m_3 \\ m_4 \\ m_5 \\ m_6 \\ m_7 \\ m_8 \\ m_9 \end{pmatrix}$$

- Fehlerstellen entfernen

Rekonstruktion der Nachricht

- $w = [5, 3, 6, 8, 2, 10, 2, 7, 1, 4]$
- $d(X) = (X - a^3)(X - a^8)$

$$\begin{pmatrix} a^0 \\ a^1 \\ a^2 \\ a^3 \\ a^4 \\ a^5 \\ a^6 \\ a^7 \\ a^8 \\ a^9 \end{pmatrix} \begin{pmatrix} 5 \\ 3 \\ 6 \\ 8 \\ 2 \\ 10 \\ 2 \\ 7 \\ 1 \\ 4 \end{pmatrix} = \begin{pmatrix} 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 \\ 8^0 & 8^1 & 8^2 & 8^3 & 8^4 & 8^5 & 8^6 & 8^7 & 8^8 & 8^9 \\ 8^0 & 8^2 & 8^4 & 8^6 & 8^8 & 8^{10} & 8^{12} & 8^{14} & 8^{16} & 8^{18} \\ 8^0 & 8^3 & 8^6 & 8^9 & 8^{12} & 8^{15} & 8^{18} & 8^{21} & 8^{24} & 8^{27} \\ 8^0 & 8^4 & 8^8 & 8^{12} & 8^{16} & 8^{20} & 8^{24} & 8^{28} & 8^{32} & 8^{36} \\ 8^0 & 8^5 & 8^{10} & 8^{15} & 8^{20} & 8^{25} & 8^{30} & 8^{35} & 8^{40} & 8^{45} \\ 8^0 & 8^6 & 8^{12} & 8^{18} & 8^{24} & 8^{30} & 8^{36} & 8^{42} & 8^{48} & 8^{54} \\ 8^0 & 8^7 & 8^{14} & 8^{21} & 8^{28} & 8^{35} & 8^{42} & 8^{49} & 8^{56} & 8^{63} \\ 8^0 & 8^8 & 8^{16} & 8^{24} & 8^{32} & 8^{40} & 8^{48} & 8^{56} & 8^{64} & 8^{72} \\ 8^0 & 8^9 & 8^{18} & 8^{27} & 8^{36} & 8^{45} & 8^{54} & 8^{63} & 8^{72} & 8^{81} \end{pmatrix} \cdot \begin{pmatrix} m_0 \\ m_1 \\ m_2 \\ m_3 \\ m_4 \\ m_5 \\ m_6 \\ m_7 \\ m_8 \\ m_9 \end{pmatrix}$$

- Fehlerstellen entfernen

Rekonstruktion der Nachricht

- $w = [5, 3, 6, 8, 2, 10, 2, 7, 1, 4]$
- $d(X) = (X - a^3)(X - a^8)$

$$
\begin{pmatrix} a^0 \\ a^1 \\ a^2 \\ a^3 \\ a^4 \\ a^5 \\ a^6 \\ a^7 \\ a^8 \\ a^9 \end{pmatrix}
\begin{pmatrix} 5 \\ 3 \\ 6 \\ 8 \\ 2 \\ 10 \\ 2 \\ 7 \\ 1 \\ 4 \end{pmatrix}
=
\begin{pmatrix}
8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 \\
8^0 & 8^1 & 8^2 & 8^3 & 8^4 & 8^5 & 8^6 & 8^7 & 8^8 & 8^9 \\
8^0 & 8^2 & 8^4 & 8^6 & 8^8 & 8^{10} & 8^{12} & 8^{14} & 8^{16} & 8^{18} \\
8^0 & 8^3 & 8^6 & 8^9 & 8^{12} & 8^{15} & 8^{18} & 8^{21} & 8^{24} & 8^{27} \\
8^0 & 8^4 & 8^8 & 8^{12} & 8^{16} & 8^{20} & 8^{24} & 8^{28} & 8^{32} & 8^{36} \\
8^0 & 8^5 & 8^{10} & 8^{15} & 8^{20} & 8^{25} & 8^{30} & 8^{35} & 8^{40} & 8^{45} \\
8^0 & 8^6 & 8^{12} & 8^{18} & 8^{24} & 8^{30} & 8^{36} & 8^{42} & 8^{48} & 8^{54} \\
8^0 & 8^7 & 8^{14} & 8^{21} & 8^{28} & 8^{35} & 8^{42} & 8^{49} & 8^{56} & 8^{63} \\
8^0 & 8^8 & 8^{16} & 8^{24} & 8^{32} & 8^{40} & 8^{48} & 8^{56} & 8^{64} & 8^{72} \\
8^0 & 8^9 & 8^{18} & 8^{27} & 8^{36} & 8^{45} & 8^{54} & 8^{63} & 8^{72} & 8^{81}
\end{pmatrix}
\cdot
\begin{pmatrix} m_0 \\ m_1 \\ m_2 \\ m_3 \\ m_4 \\ m_5 \\ m_6 \\ m_7 \\ m_8 \\ m_9 \end{pmatrix}
$$

- Fehlerstellen entfernen

Rekonstruktion der Nachricht

$$\begin{pmatrix} 5 \\ 3 \\ 6 \\ 2 \\ 10 \\ 2 \\ 7 \\ 4 \end{pmatrix} = \begin{pmatrix} 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 \\ 8^0 & 8^1 & 8^2 & 8^3 & 8^4 & 8^5 & 8^6 & 8^7 & 8^8 & 8^9 \\ 8^0 & 8^2 & 8^4 & 8^6 & 8^8 & 8^{10} & 8^{12} & 8^{14} & 8^{16} & 8^{18} \\ 8^0 & 8^4 & 8^8 & 8^{12} & 8^{16} & 8^{20} & 8^{24} & 8^{28} & 8^{32} & 8^{36} \\ 8^0 & 8^5 & 8^{10} & 8^{15} & 8^{20} & 8^{25} & 8^{30} & 8^{35} & 8^{40} & 8^{45} \\ 8^0 & 8^6 & 8^{12} & 8^{18} & 8^{24} & 8^{30} & 8^{36} & 8^{42} & 8^{48} & 8^{54} \\ 8^0 & 8^7 & 8^{14} & 8^{21} & 8^{28} & 8^{35} & 8^{42} & 8^{49} & 8^{56} & 8^{63} \\ 8^0 & 8^9 & 8^{18} & 8^{27} & 8^{36} & 8^{45} & 8^{54} & 8^{63} & 8^{72} & 8^{81} \end{pmatrix} \cdot \begin{pmatrix} m_0 \\ m_1 \\ m_2 \\ m_3 \\ m_4 \\ m_5 \\ m_6 \\ m_7 \\ m_8 \\ m_9 \end{pmatrix}$$

- Nullstellen entfernen

Rekonstruktion der Nachricht

$$\begin{pmatrix} 5 \\ 3 \\ 6 \\ 2 \\ 10 \\ 2 \\ 7 \\ 4 \end{pmatrix} = \begin{pmatrix} 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 \\ 8^0 & 8^1 & 8^2 & 8^3 & 8^4 & 8^5 & 8^6 & 8^7 & 8^8 & 8^9 \\ 8^0 & 8^2 & 8^4 & 8^6 & 8^8 & 8^{10} & 8^{12} & 8^{14} & 8^{16} & 8^{18} \\ 8^0 & 8^4 & 8^8 & 8^{12} & 8^{16} & 8^{20} & 8^{24} & 8^{28} & 8^{32} & 8^{36} \\ 8^0 & 8^5 & 8^{10} & 8^{15} & 8^{20} & 8^{25} & 8^{30} & 8^{35} & 8^{40} & 8^{45} \\ 8^0 & 8^6 & 8^{12} & 8^{18} & 8^{24} & 8^{30} & 8^{36} & 8^{42} & 8^{48} & 8^{54} \\ 8^0 & 8^7 & 8^{14} & 8^{21} & 8^{28} & 8^{35} & 8^{42} & 8^{49} & 8^{56} & 8^{63} \\ 8^0 & 8^9 & 8^{18} & 8^{27} & 8^{36} & 8^{45} & 8^{54} & 8^{63} & 8^{72} & 8^{81} \end{pmatrix} \cdot \begin{pmatrix} m_0 \\ m_1 \\ m_2 \\ m_3 \\ m_4 \\ m_5 \\ \color{green}{m_6} \\ \color{green}{m_7} \\ \color{green}{m_8} \\ \color{green}{m_9} \end{pmatrix}$$

- Nullstellen entfernen

Rekonstruktion der Nachricht

$$
\begin{pmatrix} 5 \\ 3 \\ 6 \\ 2 \\ 10 \\ 2 \\ 7 \\ 4 \end{pmatrix}
=
\begin{pmatrix}
8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 \\
8^0 & 8^1 & 8^2 & 8^3 & 8^4 & 8^5 & 8^6 & 8^7 & 8^8 & 8^9 \\
8^0 & 8^2 & 8^4 & 8^6 & 8^8 & 8^{10} & 8^{12} & 8^{14} & 8^{16} & 8^{18} \\
8^0 & 8^4 & 8^8 & 8^{12} & 8^{16} & 8^{20} & 8^{24} & 8^{28} & 8^{32} & 8^{36} \\
8^0 & 8^5 & 8^{10} & 8^{15} & 8^{20} & 8^{25} & 8^{30} & 8^{35} & 8^{40} & 8^{45} \\
8^0 & 8^6 & 8^{12} & 8^{18} & 8^{24} & 8^{30} & 8^{36} & 8^{42} & 8^{48} & 8^{54} \\
8^0 & 8^7 & 8^{14} & 8^{21} & 8^{28} & 8^{35} & 8^{42} & 8^{49} & 8^{56} & 8^{63} \\
8^0 & 8^9 & 8^{18} & 8^{27} & 8^{36} & 8^{45} & 8^{54} & 8^{63} & 8^{72} & 8^{81}
\end{pmatrix}
\cdot
\begin{pmatrix} m_0 \\ m_1 \\ m_2 \\ m_3 \\ m_4 \\ m_5 \\ m_6 \\ m_7 \\ m_8 \\ m_9 \end{pmatrix}
$$

- Nullstellen entfernen

Rekonstruktion der Nachricht

$$\begin{pmatrix} 5 \\ 3 \\ 6 \\ 2 \\ 10 \\ 2 \\ 7 \\ 4 \end{pmatrix} = \begin{pmatrix} 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 \\ 8^0 & 8^1 & 8^2 & 8^3 & 8^4 & 8^5 \\ 8^0 & 8^2 & 8^4 & 8^6 & 8^8 & 8^{10} \\ 8^0 & 8^4 & 8^8 & 8^{12} & 8^{16} & 8^{20} \\ 8^0 & 8^5 & 8^{10} & 8^{15} & 8^{20} & 8^{25} \\ 8^0 & 8^6 & 8^{12} & 8^{18} & 8^{24} & 8^{30} \\ 8^0 & 8^7 & 8^{14} & 8^{21} & 8^{28} & 8^{35} \\ 8^0 & 8^9 & 8^{18} & 8^{27} & 8^{36} & 8^{45} \end{pmatrix} \cdot \begin{pmatrix} m_0 \\ m_1 \\ m_2 \\ m_3 \\ m_4 \\ m_5 \end{pmatrix}$$

- Matrix in eine Quadratische Form bringen

Rekonstruktion der Nachricht

$$\begin{pmatrix} 5 \\ 3 \\ 6 \\ 2 \\ 10 \\ 2 \\ 7 \\ 4 \end{pmatrix} = \begin{pmatrix} 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 \\ 8^0 & 8^1 & 8^2 & 8^3 & 8^4 & 8^5 \\ 8^0 & 8^2 & 8^4 & 8^6 & 8^8 & 8^{10} \\ 8^0 & 8^4 & 8^8 & 8^{12} & 8^{16} & 8^{20} \\ 8^0 & 8^5 & 8^{10} & 8^{15} & 8^{20} & 8^{25} \\ 8^0 & 8^6 & 8^{12} & 8^{18} & 8^{24} & 8^{30} \\ 8^0 & 8^7 & 8^{14} & 8^{21} & 8^{28} & 8^{35} \\ 8^0 & 8^9 & 8^{18} & 8^{27} & 8^{36} & 8^{45} \end{pmatrix} \cdot \begin{pmatrix} m_0 \\ m_1 \\ m_2 \\ m_3 \\ m_4 \\ m_5 \end{pmatrix}$$

- Matrix in eine Quadratische Form bringen

Rekonstruktion der Nachricht

$$\begin{pmatrix} 5 \\ 3 \\ 6 \\ 2 \\ 10 \\ 2 \end{pmatrix} = \begin{pmatrix} 8^0 & 8^0 & 8^0 & 8^0 & 8^0 & 8^0 \\ 8^0 & 8^1 & 8^2 & 8^3 & 8^4 & 8^5 \\ 8^0 & 8^2 & 8^4 & 8^6 & 8^8 & 8^{10} \\ 8^0 & 8^4 & 8^8 & 8^{12} & 8^{16} & 8^{20} \\ 8^0 & 8^5 & 8^{10} & 8^{15} & 8^{20} & 8^{25} \\ 8^0 & 8^6 & 8^{12} & 8^{18} & 8^{24} & 8^{30} \end{pmatrix} \cdot \begin{pmatrix} m_0 \\ m_1 \\ m_2 \\ m_3 \\ m_4 \\ m_5 \end{pmatrix}$$

- Matrix Invertieren

Rekonstruktion der Nachricht

$$\begin{pmatrix} 5 \\ 3 \\ 6 \\ 2 \\ 10 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 8 & 9 & 6 & 4 & 10 \\ 1 & 9 & 4 & 3 & 5 & 1 \\ 1 & 4 & 5 & 9 & 3 & 1 \\ 1 & 10 & 1 & 10 & 1 & 10 \\ 1 & 3 & 9 & 5 & 4 & 1 \end{pmatrix} \cdot \begin{pmatrix} m_0 \\ m_1 \\ m_2 \\ m_3 \\ m_4 \\ m_5 \end{pmatrix}$$

$$\Downarrow$$

$$\begin{pmatrix} m_0 \\ m_1 \\ m_2 \\ m_3 \\ m_4 \\ m_5 \end{pmatrix} = \begin{pmatrix} 6 & 4 & 4 & 6 & 2 & 1 \\ 2 & 7 & 10 & 3 & 4 & 7 \\ 1 & 8 & 9 & 8 & 3 & 4 \\ 3 & 6 & 6 & 4 & 5 & 9 \\ 10 & 10 & 9 & 8 & 1 & 6 \\ 1 & 9 & 6 & 4 & 7 & 6 \end{pmatrix} \cdot \begin{pmatrix} 5 \\ 3 \\ 6 \\ 2 \\ 10 \\ 2 \end{pmatrix}$$

Rekonstruktion der Nachricht

$$\begin{pmatrix} m_0 \\ m_1 \\ m_2 \\ m_3 \\ m_4 \\ m_5 \end{pmatrix} = \begin{pmatrix} 6 & 4 & 4 & 6 & 2 & 1 \\ 2 & 7 & 10 & 3 & 4 & 7 \\ 1 & 8 & 9 & 8 & 3 & 4 \\ 3 & 6 & 6 & 4 & 5 & 9 \\ 10 & 10 & 9 & 8 & 1 & 6 \\ 1 & 9 & 6 & 4 & 7 & 6 \end{pmatrix} \cdot \begin{pmatrix} 5 \\ 3 \\ 6 \\ 2 \\ 10 \\ 2 \end{pmatrix}$$

- $m = [4, 7, 2, 5, 8, 1]$