>CypherMatrix< Verschlüsselungen

Das **CypherMatrix** Verfahren bewirkt die Verschlüsselung mit der Kombination folgender Operationen:

XOR Verknüpfung	**XOR**	D, 4, b
Substitution dyn24	**dyn24**	D, 4, c
Bit conversion (8 bit → 7 bit)	**BC(8/7)**	D, 4, d (2)
Bit conversion (8 bit → 9 bit)	**BC(8/9)**	D, 4, d (4)
Bit conversion (8 bit → 6 bit)	**coding base 64**	D, 4, d (1)
Struktur changing	**SC**	D, 4, d (3)
Zahlensystem Basis 4	**BC4**	D, 4, d (5)
Regression Reg	**Reg**	D, 4, d (6)
Bit exchange	**BE**	D, 4, e (1,2)
erweiterte Bitfolgen	**SBE**	D, 4, e (3)
Bit crossing	**BCR**	D, 4, f
Zahlensystem Basis 256	**B256**	D, 4, g
Byte Transposition	**BT**	D, 4, h
multi-time-pad	**MtP**	D, 4, j

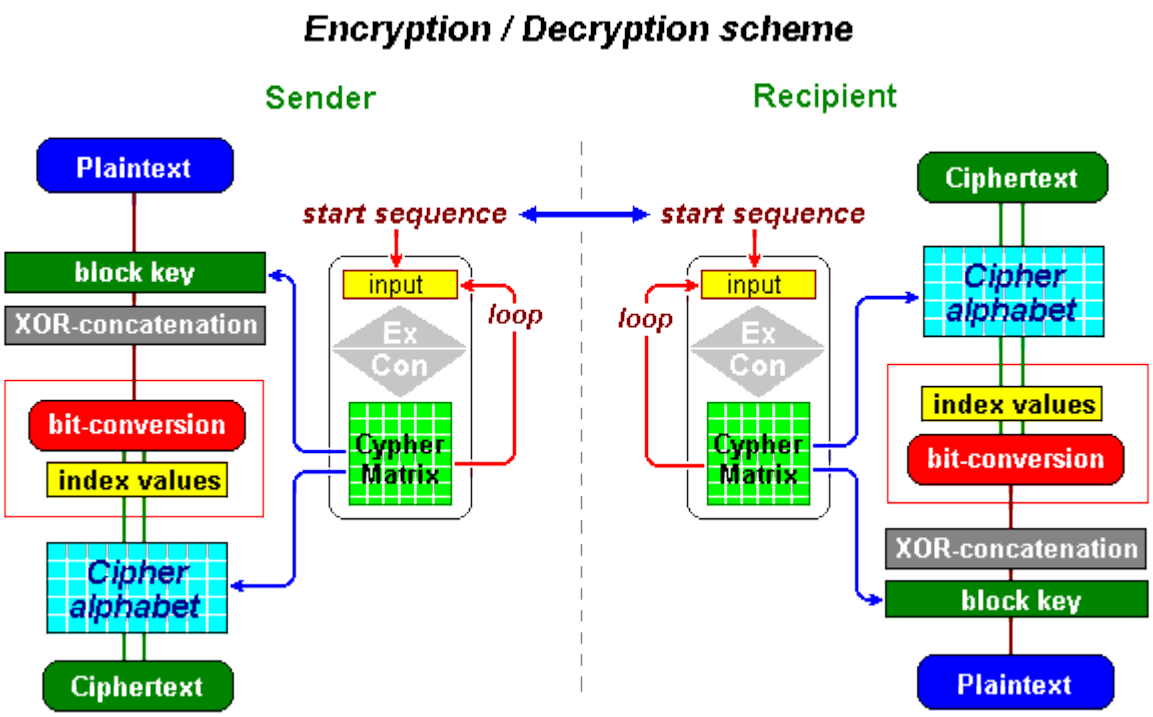
Die rechte Spalte bezeichnet die Textstellen im WEB-Artikel:

CYPHKERN.HTM Digitale Verschlüsselungen

Die Verschlüsselung als symetrisches Verfahren wird von den vorstehenden Operationen einzeln oder in Kombination durchgeführt. Eine >start sequence<von optimal 42 Bytes steuert den gesamten Verlauf sowohl beim Sender als auch beim Empfänger. Für jedes Programm sind die folgenden Parameter erforderlich:

Länge des >Matrix-Schlüssels< :	36 – 64 Bytes
Länge des Block-Schlüssels :	35 – 96 Bytes
Zahlensystem für Expansionsfunktion:	35 – 96 Grundziffern
individueller Anwender-Code:	1 – 99 Zahl

Das folgende Schema zeigt die Zusammenhänge:



Alle weiteren Einzelheiten finden Sie im Internet unter:

http://www.telecypher.net/CYPHKERN.HTM

Mit den aufgeführten Operationen werden folgende Programme gestaltet:

Hauptprogramme

CYPHER	**XOR – dyn24 - BC(8/7)**
CYPHERXT	**XOR - BC(8/7)**

Einfache Operation

CYPHER11	**XOR**
CYPHER12	**dyn24**
CYPHER13	**BC(8/7)**
CYPHER14	**BE**
CYPHER15	**CR**
CYPHER16	**BC4**
CYPHER17	**SC**
CYPHER18	**BCR**
CYPHER 51	**BT**
CYPHER55	**SBE**
CYPHER64	**coding base 64**

CYPHER89	**BC(8/9)**
CYPHER97	**B256**
CYPHER98	**B256**
CYPHER99	**B256**

Zweifache Kombinationen

CYPHER19	**BC(8/7) – Reg**
CYPHER20	**dyn24 – BE**
CYPHER21	**XOR - dyn24**
CYPHER22	**XOR - BC(8/7)**
CYPHER23	**dyn24 - XOR**
CYPHER24	**dyn24 - BC(8/7)**
CYPHER25	**BC(8/7) - XOR**
CYPHER26	**BC(8/7) - dyn24**
CYPHER27	**BE - XOR**
CYPHER28	**BE - BC(8/7)**
CYPHER29	**XOR - BCR**
CYPHER44	**dyn24 - BC(8/7)**
CYPHER52	**BT - dyn24**
CYPHER56	**SBE - BC(8/7)**
CYPHER59	**BE - SBE**
CYPHER61	**XOR - BC4**
CYPHER71	**XOR - SC**
CYPHER81	**SC - BC(8/7)**
CYPHER90	**BC(8/7) - Reg**
CYPHER91	**BC(8/7) - Reg**
CYPHER94	**BC(8/7) - Reg**

Dreifache Kombinationen

CYPHER31	**XOR – dyn24 - BC(8/7)**
CYPHER32	**XOR – BC(8/7) - dyn24**
CYPHER33	**dyn24 – XOR - BC(8/7)**
CYPHER34	**dyn24 – BC(8/7) - XOR**
CYPHER35	**BC(8/7) – XOR - dyn24**
CYPHER36	**BC(8/7) – dyn24 - XOR**
CYPHER37	**BE – XOR - BC(8/7)**
CYPHER38	**BE – BC(8/7) - XOR**
CYPHER39	**BE – dyn24 - BCR**
CYPHER53	**BT – dyn24 - BC(8/7)**
CYPHER57	**SBE – dyn24 - BC(8/7)**
CYPHER5B	**SBE – BCR - Reg**

CYPHER5C	**BT – dyn24 - XOR**
CYPHER62	**BE – dyn24 - BC4**
CYPHER63	**SBE – dyn24 - BC4**
CYPHER72	**XOR – dyn24 - SC**
CYPHER82	**MtP (SC – dyn24 - XOR)**
CYPHER83	**SC – dyn24 - BC(8/7)**
CYPHER92	**XOR – BC(8/7) - Reg**
CYPHER93	**dyn24 – BC(8/7) - Reg**

Vierfache Kombinationen

CYPHER41	**BE – XOR – dyn24 - BC(8/7)**
CYPHER42	**BE – dyn24 – XOR - BC(8/7)**
CYPHER43	**BE – dyn24 – XOR - SC**
CYPHER54	**BT – dyn24 – BC(8/7) - Reg**
CYPHER58	**SBE – XOR – BC(8/7) - Reg**
CYPHER5A	**BE – dyn24 – XOR - SBE**

Download Versionen

CYPHER-SC	**XOR - SC**	D, 4, d (3)
RECYPHER	**XOR – BC(8/7) – Reg**	D, 4, d (6)
BECYPHER	**BE – BC(8/7)**	D, 4, e (2)
SBCYPHER	**SBE – dyn24 – BC(8/7)**	D, 4, e (3)
BTCYPHER	**BT – dyn24 - BC(8/7)**	D, 4, h
MTCYPHER	**MtP**	D, 4, j

Infolge der **Bit-Konversion** >**BC(8/7)**< und dadurch fehlender „Längenkongruenz“ können alle herkömmlichen Angriffe gegen das CypherMatrix Verfahren nicht zum Erfolg führen und auch der einzig verbleibende „brute force“ Angriff ist aussichtslos (vgl: telecypher.net/CYPHKERN.HTM/Kryptanalyse).

Angriffe auf Seitenbereiche: "Side Channel Attacks"

Angriffe auf Seitenbereiche des Verfahrens Artikel: "Side Channel Attacks" sind darauf angelegt, aus arteigenen technischen Begleiterscheinungen bei der Durchführung der Entschlüsselung Rückschlüsse auf einzelne Bits, insbesondere auf verwendete Schlüssel zu gewinnen. Als verfahrenstypische Nebenbereiche dienen insbesondere:

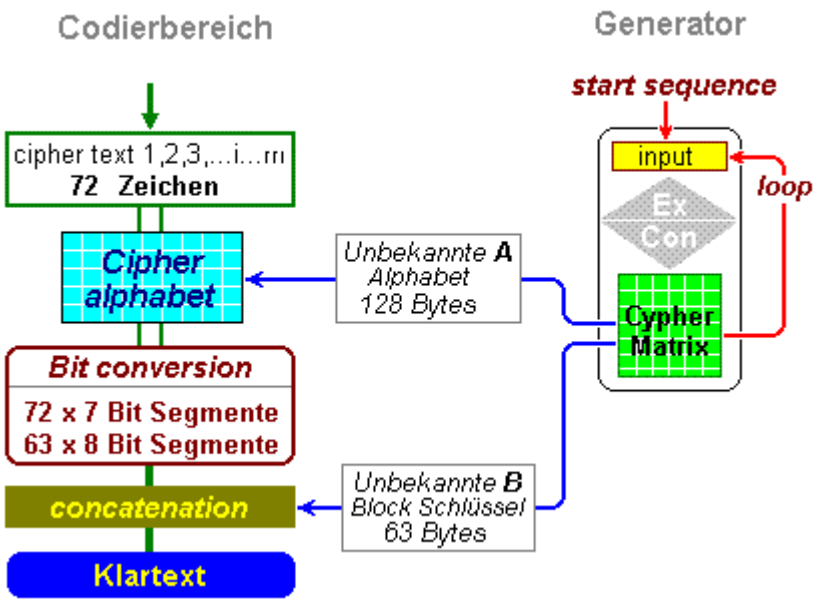
1. Analyse der Laufzeiten verschiedener Verfahrensschritte (timming attack),

2. Energieverbrauch während kryptographischer Berechnungen um Rückschlüsse auf den verwendeten Schlüssel zu erhalten (power consumption analysis),
3. Reaktionen auf falsche Eingaben (differential fault analysis)
4. und die bei Durchführung der Prozesse möglicherweise erzeugten elektromagnetischen Abstrahlungen (TEMPEST).

Ein Angreifer kennt nur den Chiffretext und das CypherMatrix Verfahren. Das jeweilige Programm und die einzelnen Steuerungsparameter, einschließlich der **Start Sequenz**, sind ihm nicht bekannt.

Die **side channel attacks** richten sich insbesondere darauf, einzelne Bits zu finden, aus denen dann weitere Folgerungen gezogen werden könnten. Das CypherMatrix Verfahren arbeitet jedoch fast ausschließlich mit Bytes (Byte-Technologie). Verfahrensrelevante Bits sind nicht vorhanden.

Die Entschlüsselung geschieht in jedem Durchgang wie folgt:



Im Chiffretext - abgearbeitet in Durchgängen von beispielsweise 72 Zeichen - sind weder Bits noch Bytes des ursprünglichen Klartextes enthalten. Die Zeichen sind auch nur Zeiger (pointers) auf Positionen im Chiffre-Alphabet. Außerdem enthält der Chiffretext keine Daten der Startsequenz oder andere Hinweise auf das Programm und seine Steuerungsparameter. Im Bereich des Generators werden ebenfalls keine Daten oder Eigenarten des Klartextes verwendet. Allein die Startsequenz am Beginn des

Prozesses steuert das gesamte Verfahren (Verfahrensgenerator).

Die zur Entschlüsselung erforderlichen Unbekannten **A** und **B** werden während des Durchgangs jeweils neu erzeugt. Daher sind auch nach einem Durchgang keine Daten gespeichert, die Ziel von side channel attacks werden könnten. Nach allem bleibt festzustellen, dass die Durchführung des CypherMatrix Verfahrens keinen Raum für Angriffe auf Seitenbereiche bietet.

Bei Interesse und zur weiteren Beschäftigung mit der Materie können einzelne Programme per e-mail beim Autor angefordert oder von der bezeichneten WEB-Seite herunter geladen werden.

mailto:eschnoor@multi-matrix.de

München, im April 2009

Ernst Erich Schnoor
München
