Blockchiffren Teil 4

Krypto II

VL 14

19.11.2018

TOTAL CYBERSECURITY JOB OPENINGS

313,735

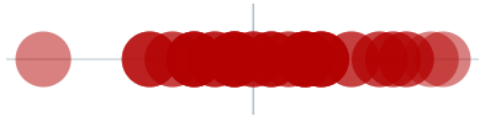
TOTAL EMPLOYED CYBERSECURITY WORKFORCE

715,715

SUPPLY OF CYBERSECURITY WORKERS

Very Low

CYBERSECURITY WORKFORCE SUPPLY/DEMAND RATIO



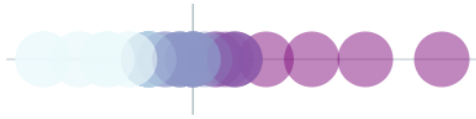
National average

2.3

GEOGRAPHIC CONCENTRATION

Average

LOCATION QUOTIENT



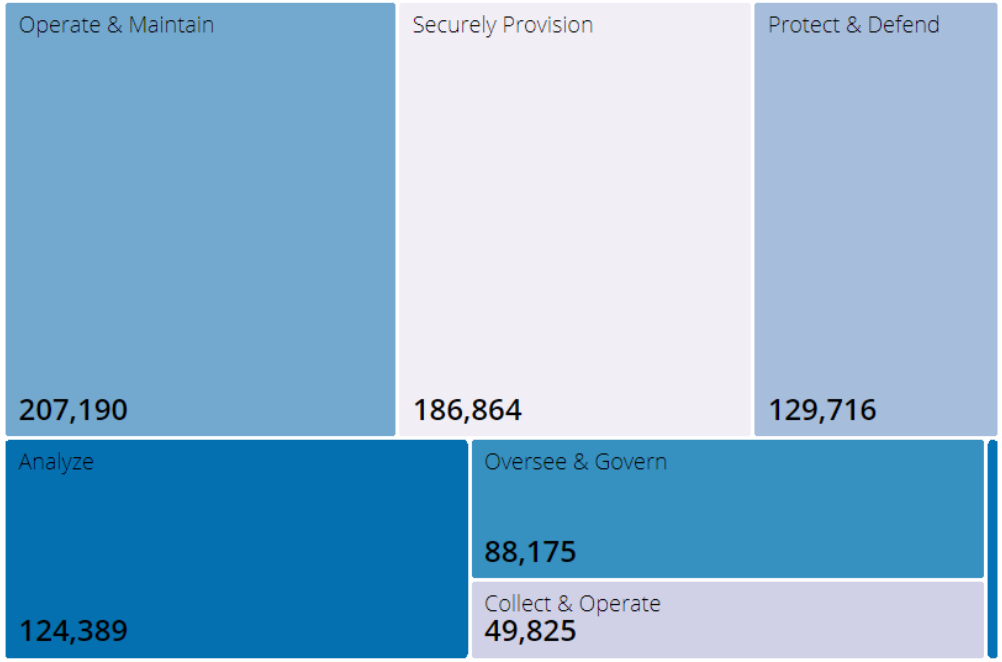
National average

1.0

TOP CYBERSECURITY JOB TITLES

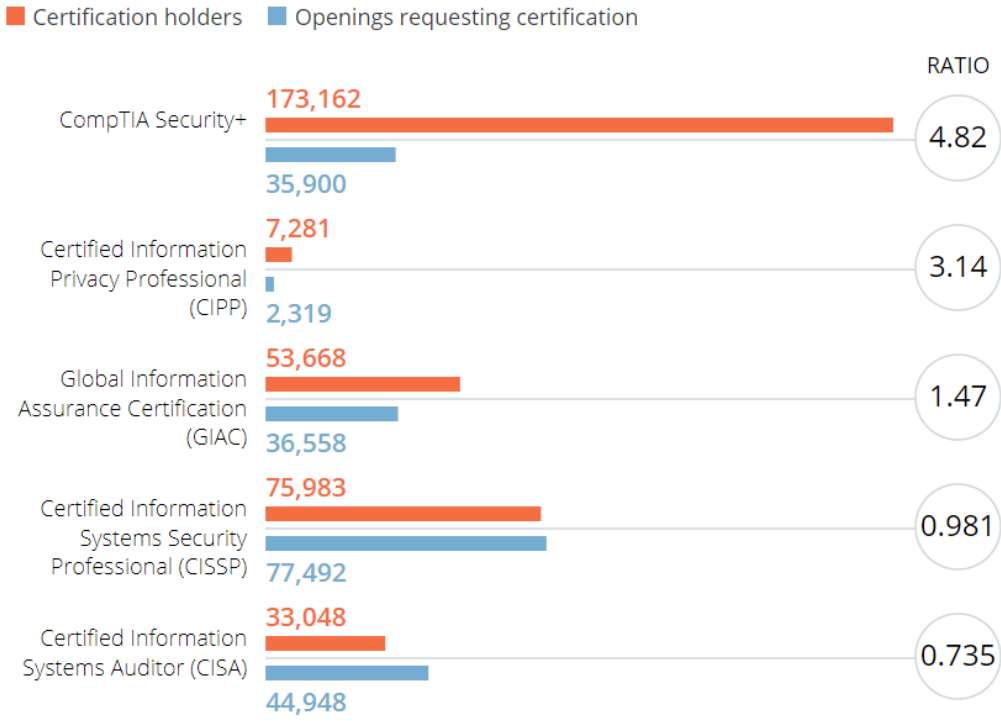
- Cyber Security Engineer
- Cyber Security Analyst
- Network Engineer / Architect
- Cyber Security Manager / Administrator
- Systems Engineer
- Software Developer / Engineer
- Systems Administrator
- Vulnerability Analyst / Penetration Tester
- Cyber Security Consultant

JOB OPENINGS BY NICE CYBERSECURITY WORKFORCE FRAMEWORK CATEGORY



Note: The Investigate category usually has fewer openings than other categories and may not be visible in the chart. To view data for the Investigate category, please hover over the thin line in the bottom right

CERTIFICATION HOLDERS / OPENINGS REQUESTING CERTIFICATION



Buch des Tages

Titel: The Block Cipher Companion

Autor(en): Lars Knudsen, Matthew Robshaw

Verlag: Springer (1. Auflage 2011)

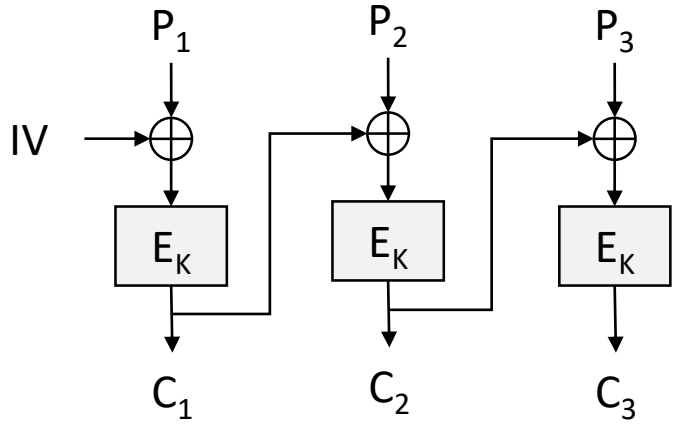
Umfang: ca. 260 Seiten

Hinweise zum Inhalt:

Dies ist eines der wenigen Fachbücher, die sich ausschließlich mit Blockchiffren beschäftigen. Die Autoren sind ausgewiesene Experten auf diesem Gebiet. DES und AES werden sehr ausführlich dargestellt, andere Blockchiffren etwas knapper. Gut und verständlich geschrieben, aber es fehlen zahlreiche Aspekte, die in den vergangenen Jahrzehnten bei der Analyse von Blockchiffren verwendet wurden. Eine gute Einführung also, aber kein Kompendium rund um die Sicherheit und das Design von Blockchiffren.

Mache OFB aus CBC

Angenommen, wir haben eine effiziente CBC-Implementierung, doch wir möchten OFB realisieren.



Wählen wir als Plaintext Input für CBC stets den Nullvektor, so wird der CBC Mode zum OFB Mode!

IEEE P1619 “Data at Rest” (1)

Die Auswahl des jeweils passendsten Betriebsmodus ist abhängig vom Einsatzszenario. Für die Verschlüsselung von Daten in Speichermedien (“Data at rest”) finden sich mehrere Anforderungskataloge. Einer davon ist IEEE P1619 und formuliert die folgenden Annahmen/Charakteristika und Anforderungen:

Annahmen:

Der Ciphertext kann von Angreifern zugegriffen werden, z.B. wie folgt:

- Einträge einer Datenbank sind verschlüsselt; alle User können auf die Datenfelder zugreifen, doch nur manche User können diese auch entschlüsseln.
- Ein Angreifer verschafft sich unbefugten Zugriff auf die verschlüsselten Daten.
- Ein verschlüsselter Datenträger wird entwendet.

IEEE P1619 “Data at Rest” (2)

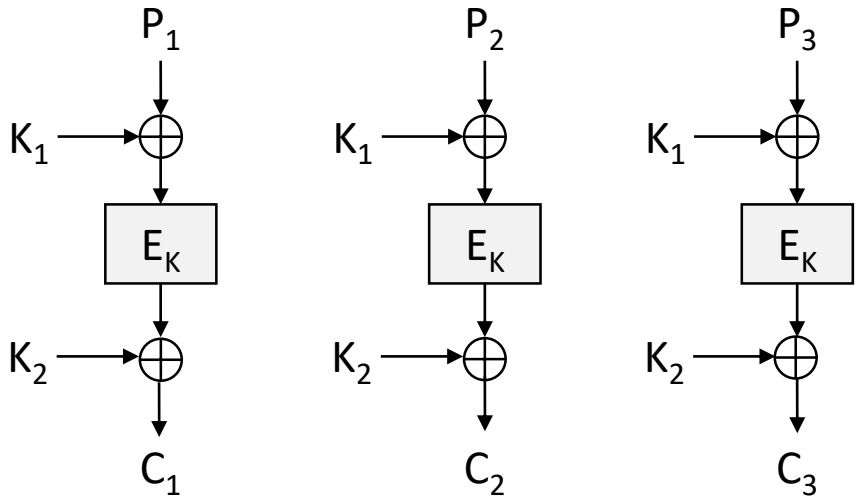
Anforderungen:

- Der Ciphertext hat identische Länge und Format wie der Plaintext.
- Die Datenblock können unabhängig voneinander individuell zugegriffen werden.
- Verschlüsselung erfolgt in voneinander unabhängigen Blocks zu je 16 Bytes (128 Bit), mit möglicher Ausnahme der beiden letzten Blöcke eines Sektors, falls der letzte Plaintext block weniger als 128 Bit Nutzdaten umfasst.
- Außer der Datenposition werden keine weiteren Metadaten zur Verschlüsselung benötigt.
- Identische Plaintexts werden auf unterschiedliche Ciphertexts abgebildet, sofern diese an unterschiedlichen Speicherorten abgelegt werden. Wird ein Plaintext wiederholt auf demselben Speicherort als Ciphertext abgelegt, so ist der Ciphertext stets derselbe.
- Ver- und Entschlüsselungsmodule müssen in der Lage sein, Daten zu entschlüsseln, die von anderen Modulen verschlüsselt wurden.

XEX Mode (1)

Xor-Encrypt-Xor bzw. ***XEX*** ist ein Beispiel für einen sogenannten ***Tweakable mode of operation***. Das Verfahren verwendet vor der Blockchiffre ein XOR mit einem Key K_1 (“Pre-Whitening”) und nach der Blockchiffre ein weiteres XOR mit einem Key K_2 (“Post-Whitening”). Ansonsten verläuft es wie ECB, verkettet die Blocks also nicht miteinander.

Verschlüsselung: $C_i = K_1 \oplus E_K(P_i) \oplus K_2$



XEX Mode (2)

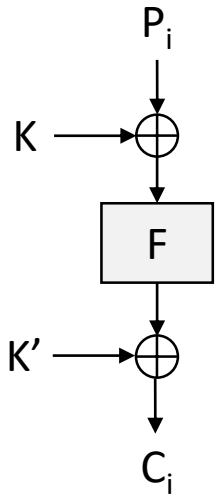
- Die meisten Betriebsmodi gibt es schon recht lange, so auch XEX. Dieser wurde 1984 vorgeschlagen von Ron Rivest, um DES besser zu schützen vor Exhaustive Search Attacks, die angesichts der DES-Schlüssellänge von 56 Bit, offenbar bereits damals einen Kritikpunkt darstellte.
- Die Verwendung von DES im XEX Mode wurde seinerzeit bezeichnet als ***DESX***.
- 1991 wurde, inspiriert durch DESX, von Even und Mansour ein anderes Blockverschlüsselungsverfahren vorgestellt, das ebenfalls mit Pre-whitening key K_1 und Post-whitening key K_2 arbeitet: die Blockchiffre DES wurde hierbei einfach ersetzt durch eine öffentlich bekannte bijektive Abbildung (Permutation).
- 2011 wurde von Dunkelman, Keller und Shamir eine Variante des oben genannten “Two-key Even-Mansour scheme” veröffentlicht, names “One-key Even-Mansour scheme”: die Autoren konnten zeigen, dass die Sicherheit des Verfahrens identisch ist, auch wenn man $K_1 = K_2$ wählt.
- XEX findet man daher ebenso als Two-key und als One-key Variante.

Even-Mansour Scheme

Two-Key Even-Mansour

Verschlüsselung:

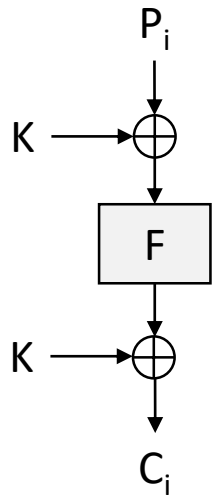
$C_i = F(K \oplus P_i) \oplus K'$



One-Key Even-Mansour

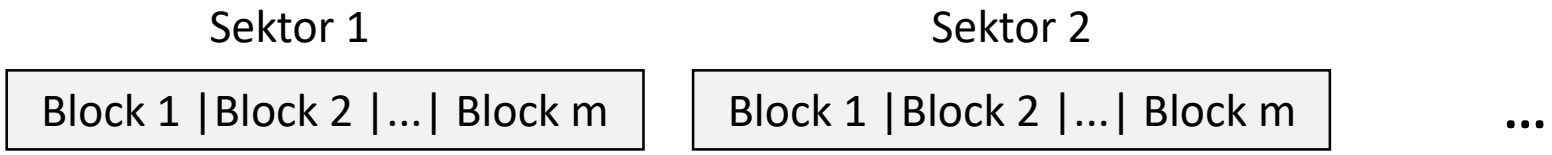
Verschlüsselung:

$C_i = F(K \oplus P_i) \oplus K$



GCM Galois Counter (1)

- Im XEX Mode stellt sich die Frage, wie man den Pre- und/oder Post-whitening key wählen soll.
- Ein prominentes Beispiel stellt der sogenannte Galois Counter (Mode) dar. Das mathematische Konstrukt wirkt auf den ersten Blick (unnötig) kompliziert, hat jedoch einige nachweisbar nützliche Eigenschaften.
- Angenommen wir verschlüsseln einen Datenträger sektorweise, dann bezeichne i die Sektornummer und j bezeichne die Blocknummer innerhalb eines Sektors.



GCM Galois Counter (2)

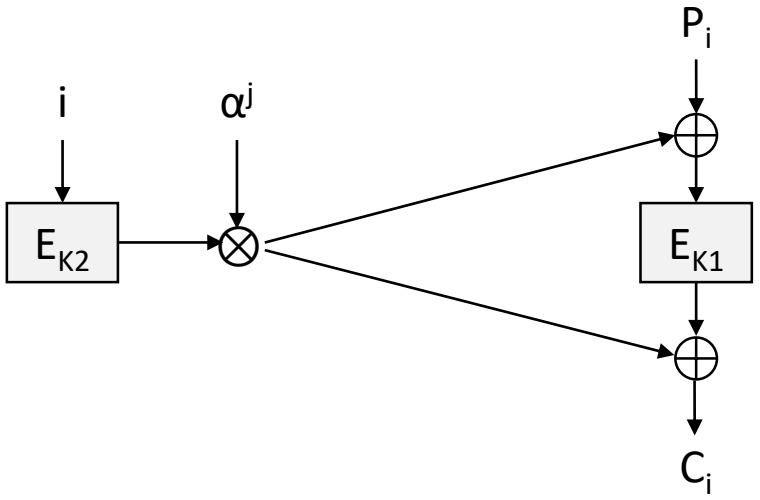
Zur Erläuterung des Galois Counters benötigen wir einige Zutaten:

- Als erstes benötigen wir ein Element $\alpha \in GF(2^{128})$, also aus dem endlichen Körper (Galois Field), dessen Elemente Polynome sind mit binären Koeffizienten.
- α soll dabei ein primitives Element sein, das korrespondiert mit dem Polynom x, bzw. in Koeffizientendarstellung: (0000...010).
- α^j bezeichne das Polynom, das entsteht durch j-fache Multiplikation von α mit sich selbst in $GF(2^{128})$.
- bitweises XOR, wie gewohnt abgekürzt mittels $\oplus$
- modulare Mutiplikation in $GF(2^{128})$, also Multiplikation zweier Polynome mit binären Koeffizienten, mit Rechnen modulo des Polynoms $x^{128} + x^7 + x^2 + x + 1$. Diese Multiplikation bezeichnen wir mit dem Symbol $\otimes$

GCM Galois Counter (3)

Warum wählt man eine so aufwendig wirkende Lösung für diesen Counter, der doch eigentlich “nur” die eindeutige Bindung des Speicherorts an den Ciphertect-Block gewährleisten soll?

Die mathematischen Hintergründe überspringen wir in diesem Fall.



XTS-AES Mode (1)

- Der sogenannte ***XTS-AES*** Mode ist ein für die Datenträgerverschlüsselung mittlerweile weit verbreitetes Verfahren, das auch standardisiert wurde in IEEE P1619, Standard Architecture for Encrypted Shared Storage Media.
- Das Verfahren kombiniert XEX, Tweaked Codebook Mode, und Ciphertext Stealing. Da die zugehörige Abkürzung XTC bereits für gleichnamige Droge verwendet wird, entschied man sich für die Abkürzung XTS...
- Der XEX Mode wird bei XTS-AES in der Version mit identischem Pre-whitening key und Post-whitening key verwendet. Dieser Key wird erzeugt im Galois Counter Mode.

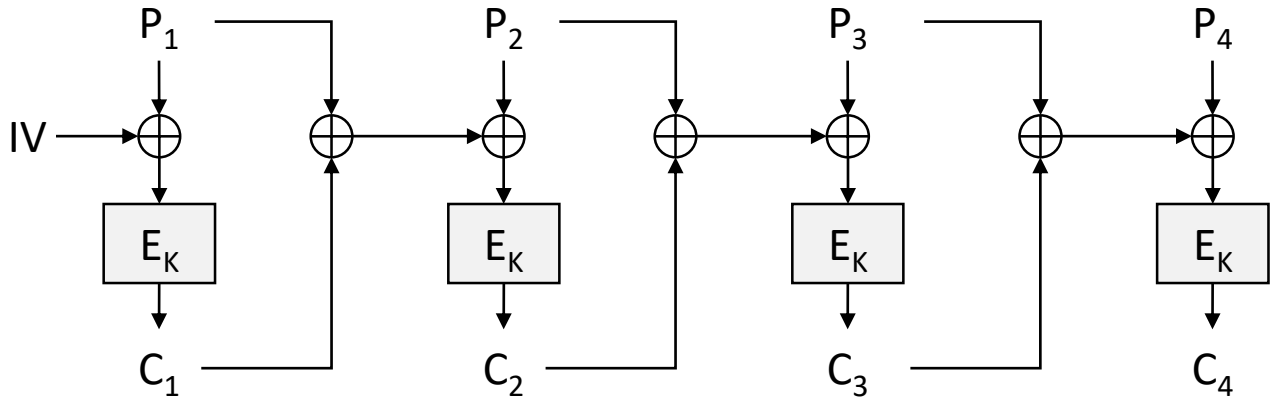
XTS-AES Mode (2)

Der XTS Mode wird (Quelle: Wikipedia) unter anderem in folgenden Anwendungen eingesetzt:

- BestCrypt
- Botan
- dm-crypt
- FreeOTFE
- TrueCrypt
- VeraCrypt
- DiskCryptor
- FreeBSD’s geli
- OpenBSD softraid disk encryption
- OpenSSL
- Mac OS X Lion’s FileVault
- Windows 10 BitLocker
- wolfCrypt

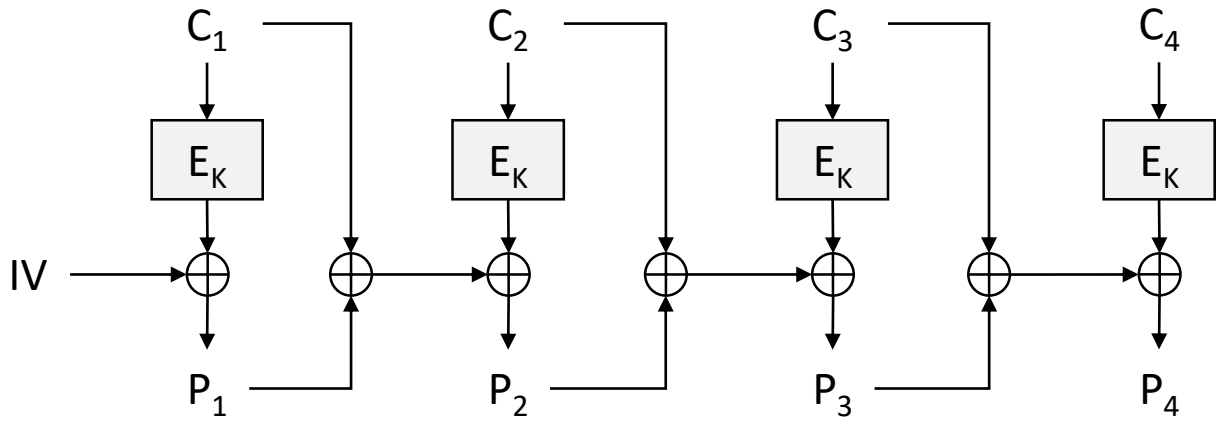
PCBC Propagating Cipher Block Chaining

Propagating Cipher Block Chaining (PCBC) ist ein weiterer Betriebsmodus. In PCBC ist keine Parallelisierung möglich, weder beim Ver- noch beim Entschlüsseln. Ebenso ist kein “Random access” möglich.



PCBC Decryption (1)

Die Entschlüsselung sehen wir anschaulich in unten stehender Graphik. Wie man sieht, führt die Veränderung eines Bits in einem Ciphertext Block dazu, dass alle nachfolgenden Blöcke zu Datensalat werden. Dies war Designziel bei PCBC.

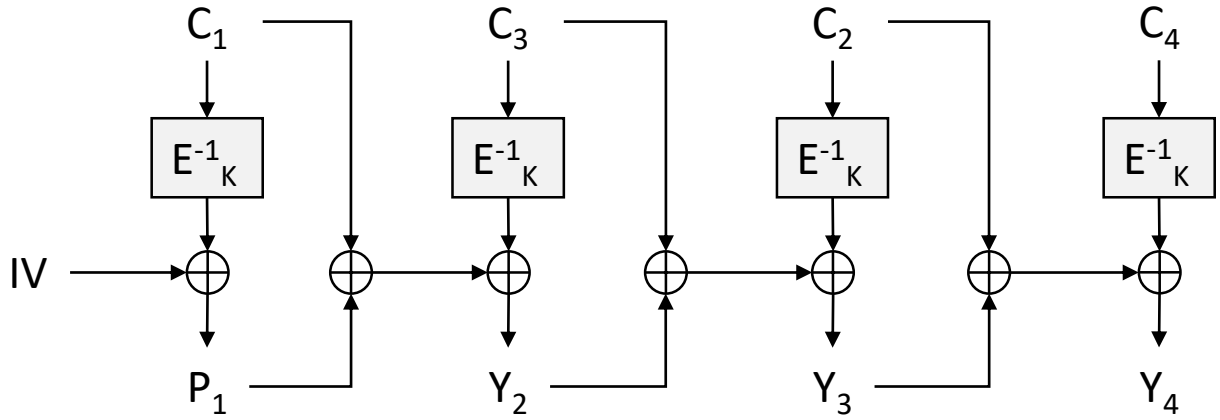


PCBC Decryption (2)

Betrachten wir nun den Fall, dass zwei benachbarte Ciphertext Blöcke (hier: C_3 und C_2) in der Reihenfolge vertauscht werden.

$Y_2 = (P_1 \oplus C_1) \oplus E^{-1}_K(C_3)$

$Y_3 = (Y_2 \oplus C_3) \oplus E^{-1}_K(C_2) = P_1 \oplus C_1 \oplus E^{-1}_K(C_3) \oplus C_3 \oplus E^{-1}_K(C_2)$



Ein korrektes bzw. reguläres P_4 hätte die Darstellung: $P_4 = (C_3 \oplus P_3) \oplus E^{-1}_K(C_4)$

PCBC Decryption (3)

Wir betrachten nun den Ciphertext Block Nr. 4 nach den Ciphertext-Blöcken Nr. 2 und 3: einmal ohne Vertauschung (also Block P_4) und einmal mit Vertauschung (also Block Y_4):

Hierfür ersetzen wir einfach nur Terme und verwenden

$P_3 = (P_2 \oplus C_2) \oplus E^{-1}_K(C_3)$, sowie $P_2 = (P_1 \oplus C_1) \oplus E^{-1}_K(C_2)$:

a) $Y_4 = (C_2 \oplus Y_3) \oplus E^{-1}_K(C_4) = C_2 \oplus Y_2 \oplus C_3 \oplus E^{-1}_K(C_2) \oplus E^{-1}_K(C_4) =$
$= C_2 \oplus P_1 \oplus C_1 \oplus E^{-1}_K(C_3) \oplus C_3 \oplus E^{-1}_K(C_2) \oplus E^{-1}_K(C_4) =$
$= P_1 \oplus C_1 \oplus C_2 \oplus C_3 \oplus E^{-1}_K(C_2) \oplus E^{-1}_K(C_3) \oplus E^{-1}_K(C_4)$

b) $P_4 = (C_3 \oplus P_3) \oplus E^{-1}_K(C_4) = P_2 \oplus C_2 \oplus E^{-1}_K(C_3) \oplus C_3 \oplus E^{-1}_K(C_4)$
$= (P_1 \oplus C_1) \oplus E^{-1}_K(C_2) \oplus C_2 \oplus E^{-1}_K(C_3) \oplus C_3 \oplus E^{-1}_K(C_4) =$
$= P_1 \oplus C_1 \oplus C_2 \oplus C_3 \oplus E^{-1}_K(C_2) \oplus E^{-1}_K(C_3) \oplus E^{-1}_K(C_4)$

PCBC Angreifbarkeit

- Es ist also $P_4 = Y_4$!
- Wir dachten, PCBC führt bei Veränderungen an einem Ciphertext dazu, dass alle nachfolgenden Datenblöcke bei einer Entschlüsselung zu Datensalat werden und eine Manipulation daher zwangsläufig auffällt.
- Offenbar kann PCBC Mode aber nicht angemessen davor schützen, dass ein Angreifer bewusst zwei benachbarte Blöcke miteinander vertauscht.
- PCBC wurde standardmäßig eingesetzt im Kerberos 4 Protokoll, ein weltweit verbreitetes Authentisierungsverfahren.
- In Kerberos 5 hat man PCBC, unter anderem wegen Bekanntwerden des obigen Schönheitsfehlers, nicht weiter eingesetzt.