Stromchiffren

Krypto II

VL 15

22.11.2018

Business Exkurs

TOTAL CYBERSECURITY JOB OPENINGS

313,735

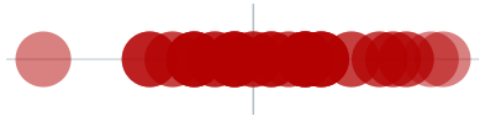
TOTAL EMPLOYED CYBERSECURITY WORKFORCE

715,715

SUPPLY OF CYBERSECURITY WORKERS

Very Low

CYBERSECURITY WORKFORCE SUPPLY/DEMAND RATIO



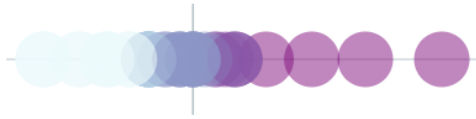
National average

2.3

GEOGRAPHIC CONCENTRATION

Average

LOCATION QUOTIENT



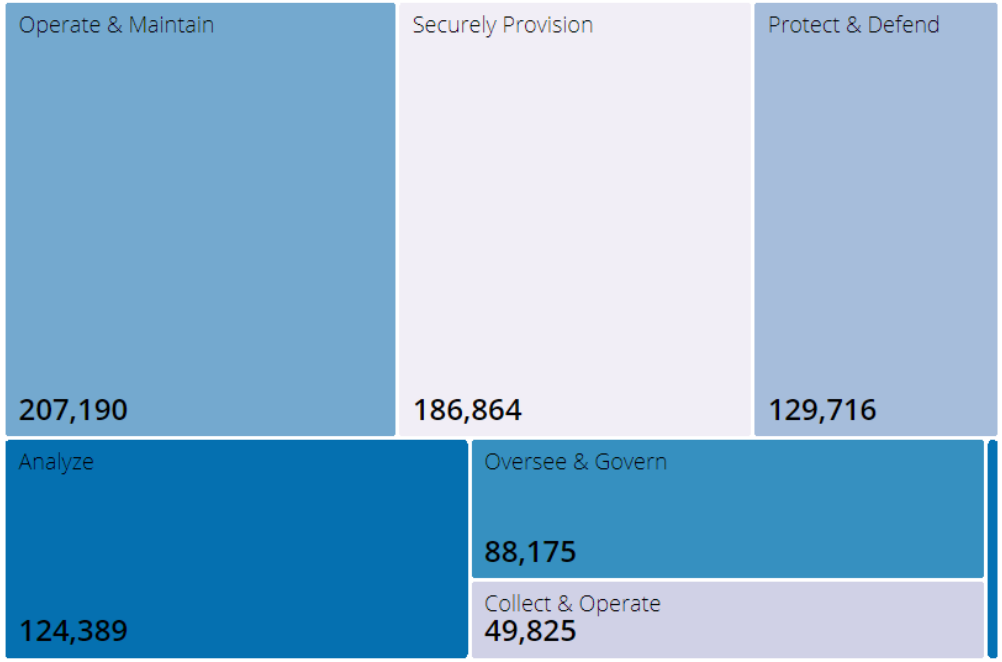
National average

1.0

TOP CYBERSECURITY JOB TITLES

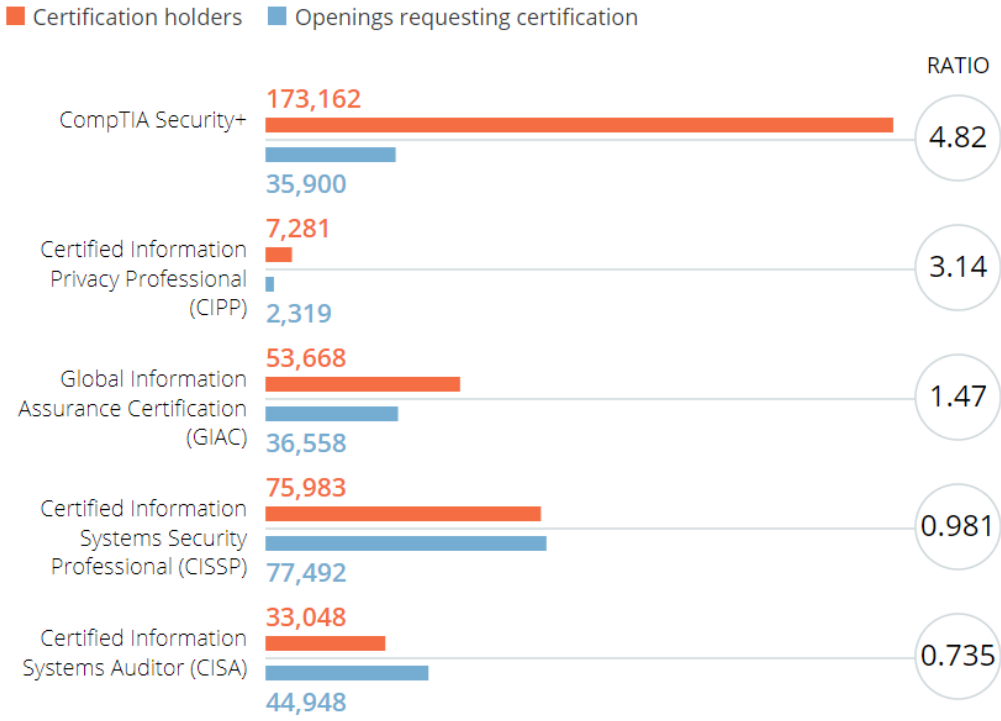
- Cyber Security Engineer
- Cyber Security Analyst
- Network Engineer / Architect
- Cyber Security Manager / Administrator
- Systems Engineer
- Software Developer / Engineer
- Systems Administrator
- Vulnerability Analyst / Penetration Tester
- Cyber Security Consultant

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



Information For

Control System Users

Information for industrial control systems owners, operators, and vendors.

Government Users

Resources for information sharing and collaboration among government agencies.

Home and Business

Information for system administrators and technical users about latest threats.

Mailing Lists and Feeds

US-CERT offers mailing lists and feeds for a variety of products including the National Cyber Awareness System and Current Activity updates. The National Cyber Awareness System was created to ensure that you have access to timely information about security topics and threats.

Subscribe to a Mailing List

To make it easier for you to receive the information, US-CERT offers four mailing lists that you can subscribe to. You may choose one or more of the following types of documents:

- **Alerts** — timely information about current security issues, vulnerabilities, and exploits
- **Analysis Reports** — in-depth analysis on new or evolving cyber threats
- **Bulletins** — weekly summaries of new vulnerabilities. Patch information is provided when available
- **Tips** — advice about common security issues for the general public
- **Current Activity** — up-to-date information about high-impact types of security activity affecting the community at large

To learn more or subscribe, visit the subscription system. and complete the process. You will need to confirm your subscription by responding to an email message that will be sent to the address you provide. If you have any questions, read the FAQ.

Feeds for Some of Our Security Documents

You can view US-CERT security documents on our website or use the below RSS feeds. You can also add these feeds to your MSN or Yahoo! homepage if you have one.

Schneier on Security

Crypto-Gram Newsletter

Crypto-Gram is a free monthly e-mail digest of posts from Bruce Schneier's Schneier on Security blog.

- Subscribe
- Unsubscribe
- Archives
- Translations
- Other Formats
- Privacy Statement

Recent Issues

November 15, 2018

In this issue:

1. How DNA Databases Violate Everyone's Privacy
2. Privacy for Tigers
3. Government Perspective on Supply Chain Security
4. West Virginia Using Internet Voting
5. Are the Police Using Smart-Home IoT Devices to Spy on People?
6. On Disguise
7. China's Hacking of the Border Gateway Protocol
8. Android Ad-Fraud Scheme
9. Detecting Fake Videos
10. Security Vulnerability in Internet-Connected Construction Cranes
11. More on the Supermicro Spying Story
12. Cell Phone Security and Heads of State
13. ID Systems Throughout the 50 States

I've been writing about security issues on my blog since 2004, and in my monthly newsletter since 1998. I write books, articles, and academic papers. Currently, I'm the Chief Technology Officer of IBM Resilient, a fellow at Harvard's Berkman Center, and a board member of EFF.

CYBER SECURITY INTERVIEWS

HOME EPISODES ABOUT CONTACT

WELCOME

Cyber Security Interviews is the weekly podcast dedicated to digging into the minds of the influencers, thought leaders, and individuals who shape the cyber security industry.

I discover what motivates them, explore their journey in cyber security, and discuss where they think the industry is going. The show lets listeners learn from the experts' stories and hear their opinions on what works (and doesn't) in cyber security.

GET STARTED WITH EPISODE ONE HERE

FEATURED EPISODES

GET STARTED WITH EPISODE ONE HERE

Öffentlichkeits-arbeit

- Presse
- Publikationen
- Newsletter
  - Anmeldung
  - Newsletter-Archive
- Ausstellungen
- Interviews
- Vorträge
- Symposium
- Downloads

Startseite < Öffentlichkeitsarbeit

Newsletter

Hier können Sie sich für den Newsletter des Bundesamtes für Verfassungsschutz und für den Wirtschaftsschutz-Newsletter anmelden.

Beide Newsletter erscheinen vier Mal im Jahr.

Um Ihr Newsletter-Abonnement abzuschließen, klicken Sie bitte auf den Link in der Bestätigungs-Mail.

Hinweistelefon islamistischer Terrorismus 0221/792-3366

Gemeinsam stark für unsere Sicherheit

Details

Güvenliğimiz İçin Hep Beraber Daha Güçlüyüz

Ayrıntılar

لندافع سويا وبصورة قوية عن أمننا وسلامتنا

التفاصيل

Publikationen

IT-Grundschutz

Newsletter

Die BSI-Newsletter versorgen Sie mit aktuellen Informationen. Aktuell stehen Ihnen folgende Newsletter zur Verfügung:

- Der BSI-Newsletter (u.a. mit Informationen zu wichtigen Themen, Veranstaltungshinweisen, Publikation,...),
- die Themen-Newsletter IT-Grundschutz und Cloud-Computing,
- sowie der Newsletter für Karriereinformationen im BSI.

Hier können Sie die › Newsletter bestellen.

IT-Grundschutz-Kataloge

IT-Grundschutz-Kataloge Downloadarchiv

IT-Grundschutz International

IT-Grundschutz-Kataloge

Inhalt

IT-Grundschutz-Kataloge Downloadarchiv

Hilfsmittel

Bezugsquellen

› **Registrierung / Newsletter**

IT-Grundschutz-Tag

IT-Grundschutz International

Prüfung

BSI untersucht Sicherheit von Windows 10

Das BSI nimmt derzeit die sicherheitsrelevanten Funktionen von Windows 10 unter die Lupe. Erste Ergebnisse befassen sich mit der Telemetrie.

312 heise online

Notfall-Patch

Adobe sichert Flash außer der Reihe ab

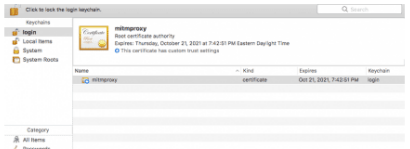
Eigentlich veröffentlicht Adobe nur ein Mal im Monat Sicherheitsupdates. Für eine gefährliche Flash-Lücke macht der Hersteller eine Ausnahme.

47

Alerts!

alle Alert-Meldungen »

- IBM Domino und Notes
- Flash
- TP-Link TL-R600VPN



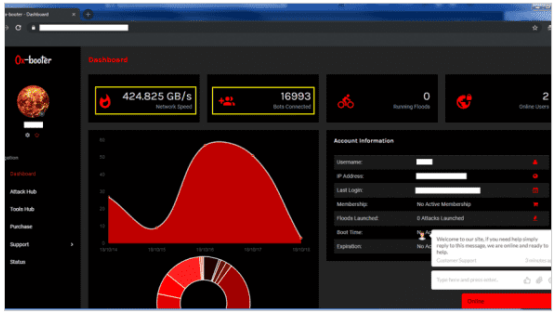
Werbe-Malware für macOS

Ein unter "SearchAwesome" und "SearchPageInjector" bekannter Datenschädling macht jetzt auf Macs die Runde. Er manipuliert Reklame und kann CPU-Zeit klauen.

Dienste

Security Consulter
Emailcheck
Netzwerkcheck
Browsercheck
Anti-Virus
Krypto-Kampagne

Artikel



Wie einfach sogar Noobs DDoS-Attacken ausführen können

Sicherheitsforscher sind auf einen Internet-Service gestoßen, über den man mit wenigen Klicks und für kleines Geld DDoS-Angriffe auf Websites starten kann. Wie einfach das geht, ist erschreckend.

Lesetipp

Newsletter heise Security Summary

Zweimal die Woche, Montags und Donnerstags, erhalten Sie eine Zusammenstellung aller sicherheitsrelevanten Ticker-Meldungen und Hintergrundberichte von heise Security. Dieser Newsletter wendet sich an alle, die nicht in Echtzeit informiert sein müssen, aber dennoch keine wichtige Info verpassen wollen. Dieser Newsletter wird im Multipart-Format, also HTML und Plaintext, verschickt.

Anmelden

Bitte geben Sie Ihre E-Mail-Adresse ein, um diesen Newsletter zu abonnieren. Wir senden Ihnen daraufhin eine E-Mail zu. Um Missbrauch auszuschließen, wird die Zusendung des Newsletters erst dann freigeschaltet, wenn Sie unsere E-Mail bestätigt haben.

E-Mail-Adresse: (Pflichtfeld)

Anrede:

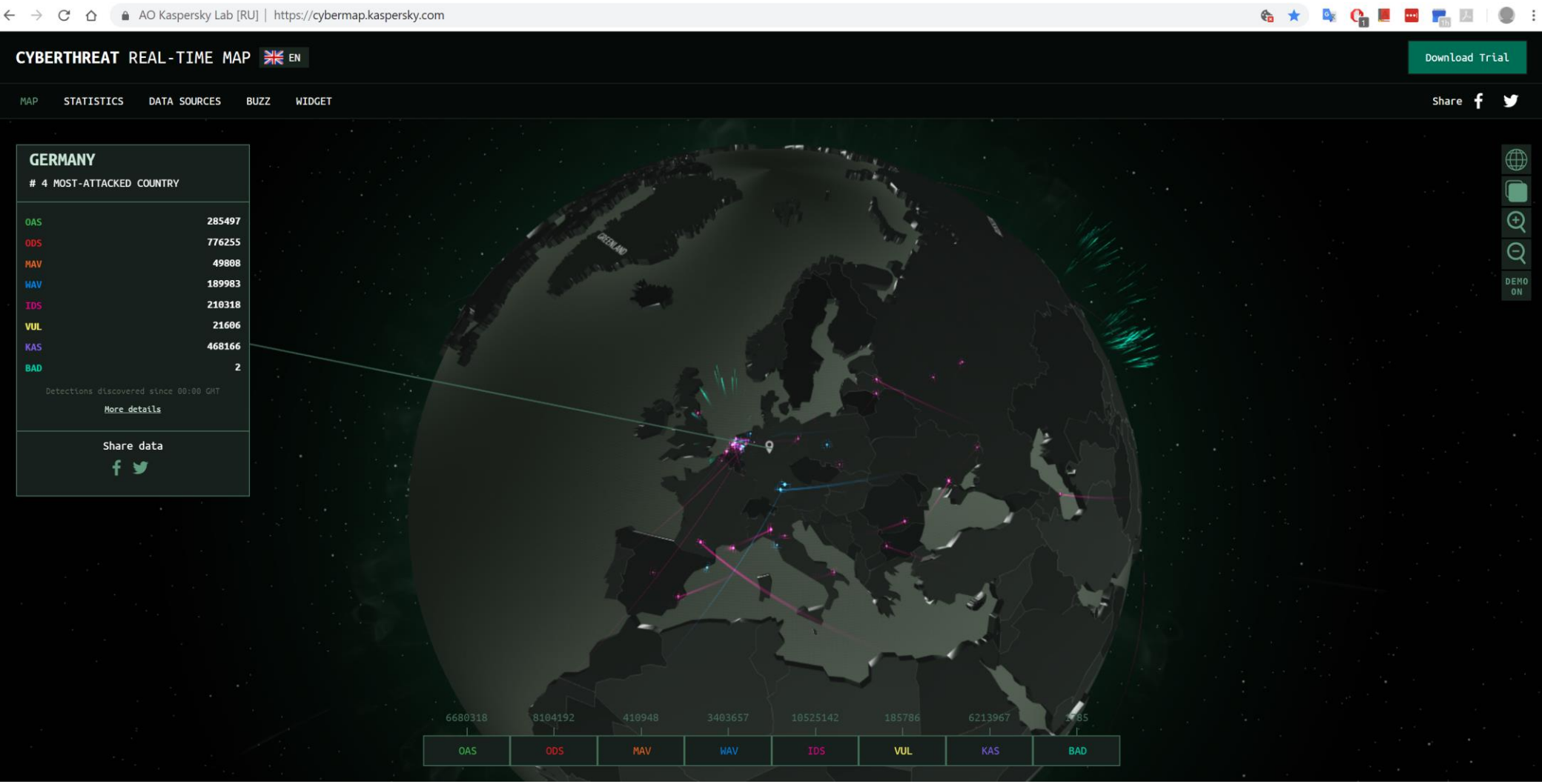
Bitte auswählen

Vorname:

Nachname:

Anmelden

https://cybermap.kaspersky.com



Buch des Tages

Titel: Angewandte Kryptographie

Autor(en): Wolfgang Ertel

Verlag: Hanser (4. Auflage 2012)

Umfang: ca. 210 Seiten

Hinweise zum Inhalt:

Dieses Buch wirbt mit dem Slogan “Auch für Nicht-Informatiker geeignet”. Zwangsläufig ist es deshalb “Für Informatiker nur bedingt geeignet”. Der Inhalt besteht aus einer Sammlung zahlreicher, teils sehr kurzer Kapitel. Diese Kapitel sind oftmals zu knapp, um dem jeweiligen Thema im Rahmen einer Kryptographie-Vorlesung gerecht zu werden. Als allererster Einstieg, beispielsweise zur Vorbereitung des Studiums oder bevor die erste Kryptographie-Vorlesung beginnt, ist das Buch aber durchaus nützlich und leicht verständlich. Als begleitendes Lehrbuch zu einer Vorlesung auf Hochschulniveau indes nur bedingt zu gebrauchen.

Aufgabe 10.1

- **Aufgabe 10.1**

Recherchieren Sie, mit welchen Verfahren die Verschlüsselung in Microsoft arbeitet, und zwar mindestens für folgende Produkte:

Windows 10 Bitlocker, Word, Excel, Powerpoint

Berücksichtigen Sie hierbei unter anderem folgende Aspekte:

- welcher Verschlüsselungsalgorithmus?
- welcher Betriebsmodus (z.B. XTS-AES oder ähnliches?)?
- wo werden die Schlüssel bzw. Passwörter abgelegt?
- welche Hashfunktionen kommen zum Einsatz?
- wie und wo werden die Schlüssel bzw. Passwörter erzeugt?
- wird Schlüsselmaterial zu Microsoft übertragen, falls ja – in welchen Einsatzszenarien?
- werden Backup-Schlüssel automatisch erzeugt?
- kann der Administrator die Daten entschlüsseln?

Aufgabe 10.2

Aufgabe 10.2

Implementieren Sie ein Programm in Python und/oder Bash, um automatisiert eine Passwort-verschlüsselte Datei durch Eingabe des in Ihrem Programm abgespeicherten, korrekten Passworts zu entschlüsseln. Die Dateiverschlüsselung soll hierbei erfolgen mithilfe von (einer oder mehreren Versionen von) zip sowie von gpg.

Anmerkung: falls Ihnen dieser Teil der Aufgabe 10.2 nicht gelingt, so gilt die Aufgabe dennoch als bestanden. Sie sollten dann aber zumindest dokumentieren, was Sie ausprobiert haben bzw. warum die Lösung dieser Aufgabe nicht geklappt hat.

Optional: Wer noch nicht genug hat: versuchen Sie es zusätzlich mit der Verschlüsselung von Adobe pdf.

Aufgabe 10.3

Aufgabe 10.3

Erweitern Sie Ihr Programm aus 10.2 wie folgt:

a) lassen Sie Ihr Programm erkennen, ob das richtige Passwort eingegeben wurde oder nicht. Liefern Sie einen Return Code zur Information an den Benutzer.

b) Verschlüsseln Sie eine Datei mit dem Passwort 1234 und testen Sie automatisiert alle vierstelligen Passwörter, bis das richtige gefunden wurde.

Dokumentation zur Aufgabe 10.x

Erstellen Sie eine Dokumentation Ihrer Lösung als pdf File. Dieses soll mindestens folgendes enthalten:

- Source Code inklusive Dokumentation als Kommentare im Code
- Konsolen-Output in Form einer simulierten bzw. abgespeicherten Session, die anzeigt, was Ihr Programm an Input und Output bezieht (ggf. auch in Form von Screenshots)
- Beschreibung der Vorgehensweise, ggf. eingebundene externe Code-Komponenten, Besonderheiten, Anmerkungen.

Deadline: Sonntag, 9. Dezember 2018 bis 23.59 Uhr

Beispiele bekannter Stromchiffren

- die meisten Verschlüsselungsmaschinen vor dem 2. Weltkrieg
- Enigma
- A5/1 und A5/2
- RC4
- Grain und Grain-128a
- One-Time Pad
- Salsa20
- Seal
- Trivium
- ...

Stromchiffren aus Blockchiffren

Wir haben bereits bei der Betrachtung von Blockcipher Operation Modes mehrere Fälle von Stromchiffren kennengelernt:

- Output Feedback Mode OFB
- Cipher Feedback Mode CFB
- Counter Mode CTR

…und weitere

Einsatzgebiete für Stromchiffren

Stromchiffren werden beispielsweise bei drahtloser Kommunikation (Mobilfunk) verwendet.

- 2G Mobilfunkstandard
- nicht 3G: dort wird eine Blockchiffre verwendet (Kasumi)
- 4G Mobilfunkstandard
- Bluetooth
- SSL

... und viele weitere

Wie funktionieren Stromchiffren (1)

- Blockchiffren verschlüsseln einen Plaintext stets blockweise. Stromchiffren hingegen verschlüsseln einen Plaintext Bit für Bit, indem sie den Datenstrom bitweise XOR-verknüpfen mit einen Schlüsselstrom.
- Eine Stromchiffre hat also ein ähnliches Funktionsprinzip wie das uns bereits bekannte One-time pad. Der Key stream einer Stromchiffre besteht allerdings nicht aus “echten” Zufallswerten, sondern errechnet sich, – wie bei einem Pseudozufallsgenerator, aus einem geheimen Startwert, dem Schlüssel der Stromchiffre.
- Für Pseudozufallsgeneratoren ist dieser geheime Startwert (Seed) die einzige Information, die zur Initialisierung benötigt wird. Bei Stromchiffren verwendet man zusätzlich noch eine Nonce als zweiten Parameter zur Initialisierung.
- Die Nonce wird bei jedem Verschlüsselungsvorgang geändert, um zu verhindern, dass zweimal derselbe Key stream erzeugt wird.
- Die Nonce kann, muss jedoch nicht geheim gehalten werden.

Wie funktionieren Stromchiffren (2)

- Typische Schlüssellängen einer Stromchiffre entsprechen jenen für Blockchiffren, also 128 Bit bis 256 Bit.
- Die Nonce hat häufig eine Länge von 64 Bit oder 128 Bit.
- Eine Nonce sollte nicht dem Risiko ausgesetzt sein, dass “versehentlich” zweimal dieselbe Nonce gewählt wird, solange der Schlüssel nicht gewechselt wurde. Anderenfalls erhält man denselben Key stream S und verschlüsselt mit diesem zwei Plaintexts P und P’:

  $C = P \oplus S$ und $C' = P' \oplus S \Rightarrow C \oplus C' = P \oplus S \oplus P' \oplus S = P \oplus P'$

  Je nach Entropie der Plaintexts kann man aus $P \oplus P'$ leicht die beiden Plaintexts P und P’ ermitteln. Kennt man einen der beiden Plaintexte, so erhält man unmittelbar den zweiten Plaintext mittels XOR.
- Bei einer zufällig gewählten Nonce der Länge 64 Bit ist bereits nach ca. 2^{32} Nonces damit zu rechnen, dass eine Wiederholung auftritt (Grund ist auch hier wieder das Birthday Paradox).

Wie funktionieren Stromchiffren (3)

Die zentrale Anforderung an den Keystream besteht darin, dass dieser pseudozufällig aussieht und nicht von einer Zufallsfolge zu unterscheiden ist.

Die den Keystream erzeugende Funktion nennt man wahlweise

- Keystream Generator
- Pseudorandom Sequence Generator
- Running Key Generator

State einer Stream Cipher

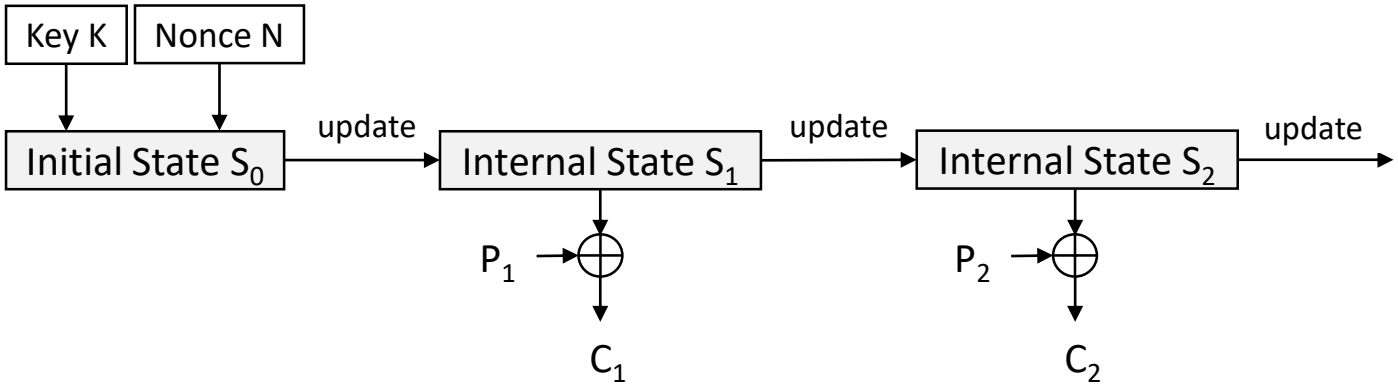
Die Gesamtheit aller Parameter (Speicherinhalte, Variablenwerte, etc.) einer Stromchiffre, deren Kenntnis es einem erlaubt, den weiteren Output bzw. Schlüsselstrom zu berechnen, bezeichnet man als ***(Internal) State*** der Stromchiffre.

Die Beschreibung einer Stromchiffre erfolgt durch Angabe des Algorithmus, wie sich der nächste Output anhand des aktuellen States berechnet.

Anmerkung: wir könnten auch von Zustand und Zustandsvariablen sprechen, doch die deutsche Übersetzung ist nicht gebräuchlich. Hierfür gibt es zu wenig deutschsprachige Literatur zu Stromchiffren.

Stateful Stream Ciphers

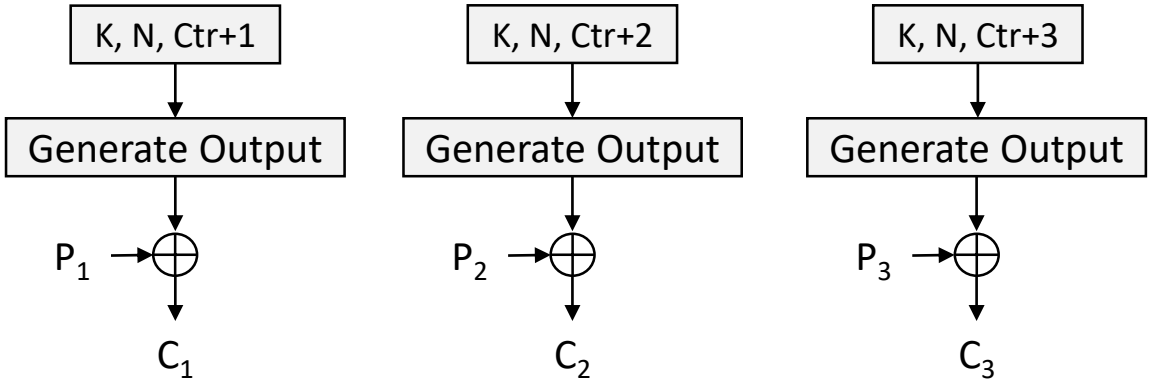
- Man unterscheidet zwischen zwei Grundtypen von Stromchiffren: Stateful und Counter-based.
- Die ***Stateful Stream Cipher*** verfügt über einen geheim zu haltenden Internal State, der während des gesamten Betriebs fortwährend modifiziert und abgespeichert werden muss.
- Der Initial State wird festgelegt durch Encryption Key und Nonce.



Counter-Based Stream Ciphers

Die ***Counter-Based Stream Cipher*** errechnet ihren Output nicht auf Grundlage eines Updates des vorherigen Internal State.

Stattdessen verwendet sie erneut den Key, die Nonce, sowie einen nach jedem Output inkrementierten Counter Ctr.



Synchronous vs Asynchronous Stream Ciphers (1)

Man unterscheidet bei Stromchiffren zwei Typen:

A. ***Synchronous Stream Cipher***: der erzeugte Schlüsselstrom hängt ausschließlich vom Key ab, nicht jedoch vom Plaintext

B. ***Asynchronous Stream Cipher***: der erzeugte Schlüsselstrom hängt nicht nur vom Key ab, sondern zusätzlich auch vom Plaintext

Synchronous vs Asynchronous Stream Ciphers (2)

Eigenschaften von Synchronous Stream Ciphers

- Fehler im Ciphertext führen bei der Entschlüsselung zu Fehlern an exakt denselben Bitpositionen im Plaintext.
- Eine Ausbreitung (Error Propagation) von Fehlern findet nicht statt, da benachbarter Plaintext oder Ciphertext nicht in die Ver- und Entschlüsselung mit eingeht.

Eigenschaften von Asynchronous Stream Ciphers

- Fehler im Ciphertext führen bei der Entschlüsselung zu Fehlern im Plaintext an derselben sowie (in Abhängigkeit vom Verfahren) an nachfolgenden Stellen.
- Ein Beispiel hierfür ist der CBC Mode.

Stromchiffren in Hardware

Oftmals wurden Stromchiffren in Hardware implementiert. Mit Hardware meinen wir hier nicht CPUs oder GPUs im PC, sondern z.B.

- Field-Programmable Gate Arrays (FPGA)
- Application-Specific Integrated Circuits (ASIC)
- Programmable Logic Devices (PLD)

Die Implementierung einer Stromchiffre benötigte früher im Vergleich zu einer Blockchiffre weniger Speicher und weniger logische Gatter. Dadurch benötigten sie insgesamt weniger Platz auf dem Integrated Circuit und waren deshalb billiger in der Herstellung.

Mittlerweile hat sich dieser Unterschied nivelliert: zum einen existieren Hardware-freundliche Blockchiffren, zum anderen sind die Kosten für Hardware insgesamt gesunken.

Feedback Shift Register (1)

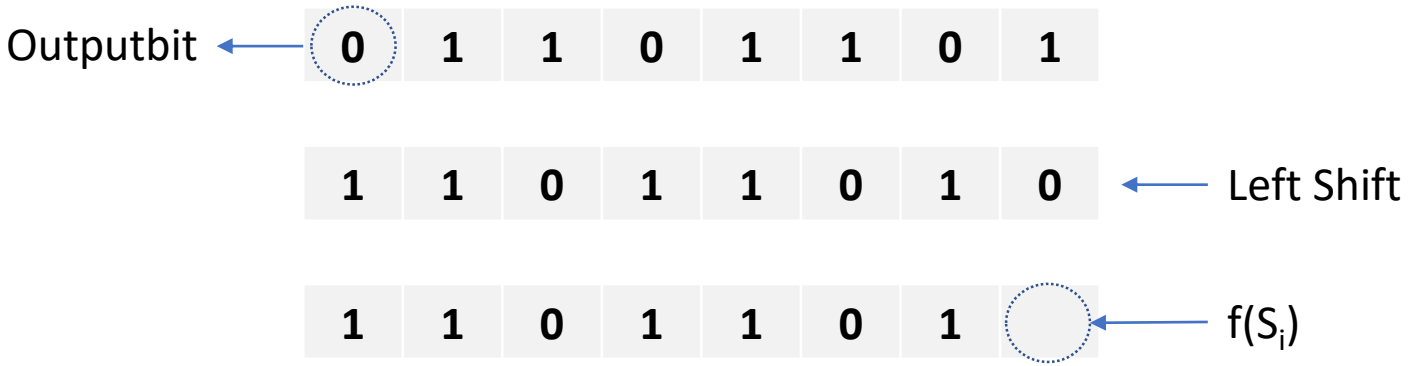
- Eine wichtige Klasse von Stromchiffren sind die sogenannten ***Feedback Shift Register FSR***. Die meisten “Hardware-Stromchiffren” sind solche FSR.
- Der Name “Feedback Shift Register” beschreibt bereits die Funktionsweise:
  - wir haben ein Register der Länge n Bit. Dieses beschreibt den aktuellen Zustand der Stromchiffre.
  - Pro Arbeitsschritt liefert das FSR ein Outputbit, in unserem Beispiel das Bit linksaußen.
  - Danach wird das Register einem Links-Shift unterzogen: das Outputbit wird linksaußen herausgeshiftet und rechtsaußen (zunächst) eine Null eingefügt.
  - Eine ***Feedback-Funktion f***: $\{0,1\}^n \rightarrow \{0,1\}$ wird auf den Registerinhalt angewandt und liefert ein Bit als Ausgabe, das im Register rechtsaußen anstelle der Null eingefügt wird.
  - Danach wiederholt sich der gesamte Vorgang.

Feedback Shift Register (2)

Beschreiben wir mit S_i das Register nach der i-ten Iteration, so lässt sich der Registerinhalt nach einem Iterationsschritt auch folgendermaßen beschreiben:

$$S_{i+1} = (S_i \ll 1) \mid f(S_i)$$

Hierbei bezeichnet $\ll 1$ einen Linksshift um eine Position, und $\mid$ steht hier nicht für Konkatenation, sondern für ein logisches Oder. Hierfür nehmen wir an, dass die Funktion f nur mit dem rechtsäußersten Bit des Registers verodert wird.



Die Feedback Shift Funktion f

- Das Verhalten unseres Feedback Shift Registers wird bestimmt von der Feedback-Funktion f.
- Die Funktion f operiert auf 2^n möglichen Registerzuständen. Ihr Output ist eine lineare oder nichtlineare Kombination der n Bits im Register.
- Lineare Funktionen f haben für kryptographische Zwecke, wie wir bereits gesehen haben, unerwünschte Eigenschaften hinsichtlich ihrer (einfachen) Berechenbarkeit. Wir betrachten diese dennoch, da sie unter anderem als Komponente komplexerer Feedback Shift Register dienen können.
- Wir bezeichnen im Folgenden den Inhalt des Registers S_i mit $S_i = (b_n, b_{n-1}, ..., b_1)$.

Beispiel für Feedback Shift Funktion (1)

Sei $f(b_8, b_7, ..., b_1) = b_8 \oplus b_7 \oplus b_6 \oplus b_5 \oplus b_4 \oplus b_3 \oplus b_2 \oplus b_1$

Der Initialwert S_1 des Registers sei $(b_8, b_7, ..., b_1) = (0, 0, 0, 0, 0, 0, 0, 1)$.

Dann erhalten wir:

$f(S_1) = 0 \oplus 0 \oplus ... \oplus 0 \oplus 1 = 1$ und

$S_2 = (b_7, b_6, ..., b_1, f(S_1)) = (0, 0, 0, 0, 0, 0, 1, 1)$

$f(S_2) = 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1 = 0$ und

$S_3 = (0, 0, 0, 0, 0, 1, 1, f(S_2)) = (0, 0, 0, 0, 0, 1, 1, 0)$

$f(S_3) = 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 0 = 0$ und

$S_4 = (0, 0, 0, 0, 1, 1, 0, f(S_3)) = (0, 0, 0, 0, 1, 1, 0, 0)$

$S_5 = (0, 0, 0, 1, 1, 0, 0, 0)$

$S_6 = (0, 0, 1, 1, 0, 0, 0, 0)$

$S_7 = (0, 1, 1, 0, 0, 0, 0, 0)$

$S_8 = (1, 1, 0, 0, 0, 0, 0, 0)$

Beispiel für Feedback Shift Funktion (2)

$S_8 = (1, 1, 0, 0, 0, 0, 0, 0)$

$S_9 = (1, 0, 0, 0, 0, 0, 0, 0)$

$S_{10} = (0, 0, 0, 0, 0, 0, 0, 1) = S_1$

Wie wir sehen, ist $S_{10} = S_1$ und wir erhalten einen Zyklus:

$S_{11} = S_2$, $S_{12} = S_3$, $S_{13} = S_4$, ..., $S_{19} = S_1$ und so weiter.

➔ In unserem Beispiel wiederholen sich die Outputbits also alle 9 Schritte. Dies nennt man die Periode.

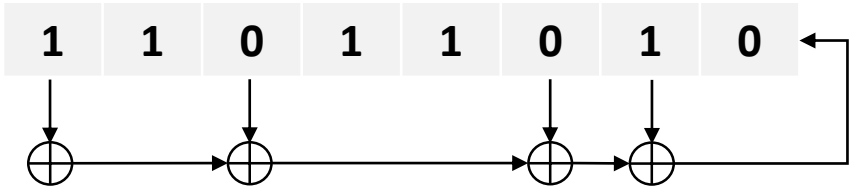
Lineare Feedback Shift Register (1)

Lineare Feedback Shift Register LFSR verwenden eine lineare Funktion f. Dies bedeutet, dass der Funktionswert gebildet wird als XOR einer Teilmenge der Bits des Registers S_i:

$f(S_i) = \sum_{j=1}^{n} a_j \cdot b_j$, wobei $a_j \in \{0,1\}$ und $S_i = (b_n, b_{n-1}, ..., b_1)$.

Anmerkung: die Summenbildung erfolgt hier also mittels XOR, und die Produkte $a_j \cdot b_j$ bezeichnen die Multiplikation in $\mathbb{Z}_2$.

Beispiel:



Lineare Feedback Shift Register (2)

- Die Wahl der a_j ist entscheidend für die Qualität eines LFSR. So wünscht man beispielsweise eine möglichst lange Periode, ohne dass sich ein Registerinhalt wiederholt.
- Die maximal mögliche Periode beträgt $2^n - 1$: das Register kann 2^n verschiedene Werte haben, wobei der Nullvektor nicht in Frage kommt, da dieser immer nur auf sich selbst abgebildet werden kann.

Maximale Periode eines LFSR

- Bei manchen FSR ist es sehr schwierig herauszufinden, welche Periode sie besitzen.
- Im Falle Linearer Feedback Shift Register jedoch kann man genau angeben, welche Bitpositionen des Registerinhalts (b_n, b_{n-1}, ..., b_1) in der linearen Feedback-Funktion f aufaddiert werden müssen, um eine maximale Periode von $2^n - 1$ zu ermöglichen:
- Hierzu interpretieren wir die Bits des Registers S_i als binäre Koeffizienten eines Polynoms $b_n x^n + b_{n-1} x^{n-1} + ... + b_1 x + 1$.

Setzen wir $b_0 = 1$, dann gilt folgender

Satz: Die Periode des LFSR ist genau dann maximal, wenn $\sum_{j=0}^{n} b_j \cdot x^j$ ein primitives Polynom ist.

Anmerkung: wir gehen an dieser Stelle nicht näher ein auf die Definition eines primitiven Polynoms. Auch beweisen wir den o.g. Satz hier nicht.