Kryptographie

In diesem kurzen Clip möchten wir Sie in die Welt der Kryptographie einführen. Da es sich um ein umfangreiches Thema handelt, soll er das Interesse für das tiefer gehende Dokument zu diesem Modul wecken.

Kryptografie bezieht sich auf Methoden zum Schutz von Informationen und Kommunikation, so dass nur diejenigen, für die die Informationen bestimmt sind, sie lesen können.

In der Informatik wird dieser Schutz mit Hilfe von Anwendungen erreicht, die komplexe mathematische Konzepte umsetzen. Diese Konzepte werden in Algorithmen kodiert, die für die kryptografische Schlüsselgenerierung, digitale Signaturen, den Schutz der Privatsphäre, das Surfen im Internet und vertrauliche Kommunikation wie E-Mail und Kreditkartentransaktionen verwendet werden.

Bei der Verschlüsselung werden die Informationen unlesbar gemacht, und bei der Entschlüsselung werden die verborgenen Informationen wiederhergestellt. Der Verschlüsselungs-/Entschlüsselungsprozess umfasst in der Regel sowohl einen Algorithmus als auch einen Schlüssel. Ein Schlüssel ist lediglich eine weitere Information, in der Regel eine Zahl, die angibt, wie der Algorithmus auf einen Klartext angewandt wird, um ihn in einen so genannten Chiffretext zu verschlüsseln. In einem sicheren kryptografischen System sollte es, selbst wenn man den zur Verschlüsselung der Nachricht verwendeten Algorithmus kennt, schwierig oder nahezu unmöglich sein, den Klartext ohne diesen Schlüssel aus dem Chiffretext wiederherzustellen.

Ein wenig Geschichte

Die Kryptografie geht auf das Jahr 2000 v. Chr. zurück, als im alten Ägypten nicht standardisierte "geheime" Hieroglyphen verwendet wurden. Im antiken Griechenland wurde insbesondere von den Spartanern ein "Gerät" namens Scytale verwendet, um während militärischer Feldzüge zu kommunizieren; es bestand aus einem Stab, um den ein Pergamentstreifen gewickelt war, auf den eine Nachricht geschrieben wurde. Der Empfänger benutzte einen Stab desselben Durchmessers, um den das Pergament gewickelt war, um die Nachricht zu lesen.

Eine etwas ausgefeiltere Methode, die moderne Methoden vorwegnimmt, ist als Caesar-Chiffre bekannt und wurde von Julius Caesar für seine vertrauliche Korrespondenz verwendet. Im Wesentlichen wird jeder Buchstabe durch einen anderen Buchstaben an einer späteren Stelle des Alphabets ersetzt, und zwar an drei Stellen. Hier können wir das Konzept des Schlüssels erkennen: wie viele Buchstaben weiter im Alphabet man gehen muss, um den Chiffretext zu erstellen. Obwohl es einfach ist und sogar in Kinderspielzeug vorkommt, berichtet Wikipedia, dass es noch in diesem Jahrhundert verwendet wurde.

Diese Art der Verschlüsselung ist einfach und kann für jede Nachricht verwendet werden. Im Gegensatz dazu steht ein System von Codewörtern, bei dem z. B. "Kauf das Buch" gleichbedeutend ist mit "Schick Legionen voraus". In diesem Fall müssen beide Seiten der Kommunikation ein gemeinsames Buch mit Codesätzen verwenden, und es gibt keine Möglichkeit, andere Sätze zu verschlüsseln.

Die Caesar-Chiffre ist eine Substitutions-Chiffre, bei der jeder Buchstabe durch einen anderen ersetzt wird; andere Varianten würden Buchstabenblöcke oder ganze Wörter ersetzen. Bis zur Mitte des vergangenen Jahrhunderts bestand die Kryptographie aus mehr oder weniger komplexen Substitutions-Chiffren, die zur Sicherung der Kommunikation von Regierungen und Militärs eingesetzt wurden. In der Zwischenzeit fanden Kryptographen immer raffiniertere Wege, um den ursprünglichen Text aus einem Chiffretext wiederherzustellen, aber vor dem Aufkommen von Computern war es schwierig, mathematische Transformationen schnell genug durchzuführen, um die Ver- und Entschlüsselung zu erleichtern. Während des Zweiten Weltkriegs setzten die Deutschen die elektromechanische Enigma-Maschine ein, um Nachrichten zu verschlüsseln, und Alan Turing leitete ein Team in Großbritannien, das eine ähnliche Maschine entwickelte, um den Code zu knacken, was auch die Grundlage für die ersten modernen Computer bildete. Mit der Verfügbarkeit von Computern wurde die Kryptografie radikal komplexer.

Für zivile Zwecke wurde die Kryptografie erst interessant, als Computer über nicht-exklusive Netzwerke miteinander verbunden wurden, da es ein Leichtes war, Daten, die über das Netzwerk übertragen wurden, auszuspionieren. Finanzdienstleistungen waren die ersten Nutzer der Netze, und für sie war es wichtig, einen Weg zu finden, Informationen geheim zu halten.

Anfang der 1970er Jahre schlug IBM den Data Encryption Standard-Algorithmus (DES) zum Schutz sensibler, nicht klassifizierter elektronischer Regierungsdaten vor. Im Jahr 1977 wurde er als offizieller Federal Information Processing Standard (FIPS) veröffentlicht und von der Industrie weitgehend übernommen. Der Algorithmus war öffentlich zugänglich.

Heute wird die öffentliche Kenntnis der kryptografischen Algorithmen als notwendig erachtet und nicht mehr als unvermeidliches Übel. Auf diese Weise können viele

erfahrene Kryptographen die Algorithmen untersuchen und Schwachstellen finden, bevor sie ausgenutzt werden..

Moderne Kryptographie

Die moderne Kryptografie verfolgt vier Ziele:

Vertraulichkeit. Die Informationen dürfen von niemandem verstanden werden, für den sie nicht bestimmt waren.

Unversehrtheit. Die Informationen können nicht verändert werden, ohne dass die Veränderung entdeckt wird.

Nicht-Abstreitbarkeit. Der Ersteller der Information kann nicht leugnen, der Ursprung der Information zu sein.

Authentifizierung. Absender und Empfänger können sich gegenseitig ihre Identität bestätigen.

In der modernen Kryptographie gilt ein wichtiger Grundsatz: das Kerckhoffs'sche Prinzip. Es besagt, dass "ein kryptografisches System auch dann sicher sein sollte, wenn alles über das System, mit Ausnahme des Schlüssels, öffentlich bekannt ist". Mit anderen Worten: Sie wollen einen Algorithmus entwickeln, der nicht geheim sein muss, um Informationen erfolgreich zu verbergen.

Types of cryptographic algorithm

Arten von kryptografischen Algorithmen

Es gibt viele kryptografische Algorithmen, aber sie lassen sich im Wesentlichen in drei Kategorien einteilen: *symmetrische Kryptografie, asymmetrische Kryptografie und Hash-Funktionen.*

Die symmetrische Kryptografie ist die typischste und älteste Familie der kryptografischen Algorithmen, an die wir in der Regel denken, wenn wir an die Verschlüsselung von Nachrichten denken. Sie werden nach der Symmetrie der Ver- und Entschlüsselungsvorgänge benannt. Diese Algorithmen verwenden einen einzigen Schlüssel, der sowohl dem Absender als auch dem Empfänger bekannt sein muss; er wird zum Verschlüsseln und Entschlüsseln einer Nachricht verwendet.

Die Caesar-Chiffre ist ein Beispiel für symmetrische Kryptographie. Was Cäsar und einer seiner Zenturionen gemeinsam wissen sollten, ist, wie viele Buchstaben sie im Alphabet vorwärts oder rückwärts bewegen müssen, um den Klartext in einen

Geheimtext zu verwandeln oder umgekehrt. Die Zahl ist bei der Verschlüsselung und bei der Entschlüsselung dieselbe, das macht sie symmetrisch.

Die symmetrische Kryptografie wird häufig verwendet, um Daten vertraulich zu halten. Sie kann nützlich sein, um eine lokale Festplatte geheim zu halten, da es in der Regel derselbe Benutzer ist, der die geschützten Daten verschlüsselt und entschlüsselt, wobei der geheime Schlüssel nicht an andere weitergegeben werden darf.

Asymmetrische Kryptographie

Asymmetrische Algorithmen verwenden nicht nur einen Schlüssel, sondern zwei: ein Schlüssel wird zur Verschlüsselung (privater Schlüssel) und der andere zur Entschlüsselung (öffentlicher Schlüssel) verwendet. Daher verwenden Sender und Empfänger beim Austausch von Nachrichten nicht denselben Schlüssel. Diese Schlüssel werden paarweise erzeugt und verwaltet: Was ein Schlüssel (irgendeiner des Paares) verschlüsselt, kann nur mit dem anderen Schlüssel des Paares entschlüsselt werden.

Der kryptografische Mechanismus, auf dem die asymmetrische Kryptografie beruht, ist der der Einwegfunktionen: mathematische Operationen, die sehr schwer umkehrbar sind. Die Multiplikation zweier sehr großer Primzahlen (z. B. des öffentlichen und des privaten Schlüssels) ist eine einfache und schnell durchzuführende Berechnung, aber es wäre sehr schwierig (in akzeptabler Zeit), die beiden ursprünglichen Primzahlen allein aus dem Ergebnis herauszufinden.

Der Grund für die Verwendung asymmetrischer Algorithmen liegt in den Problemen, die die symmetrische Kryptographie hat:

1. Eine vertrauliche Kommunikation zwischen zwei Einheiten erfordert, dass nur ein einziger Schlüssel zwischen ihnen ausgetauscht wird. Wenn die Einheiten n sind, sind $n \cdot (n-1)/2$ verschiedene Schlüssel erforderlich, um eine vertrauliche Kommunikation zwischen jedem Paar der Parteien zu ermöglichen

2. Sowohl der Sender als auch der Empfänger kennen ihren gemeinsamen Schlüssel, so dass eine Nichtabstreitbarkeit nicht möglich ist (Abstreitbarkeit ist das Bestreiten, der Urheber einer bestimmten Nachricht zu sein).

Das erste Problem ist nicht die Anzahl der Schlüssel, die jedes Subjekt zu verwalten hat, das Problem ist der Austausch dieser Schlüssel. Jedes Subjekt muss sich mit jedem der anderen n-1 Subjekte auf einen Schlüssel einigen, was in der Tat eine

komplexe Operation ist; dies macht die symmetrische Kryptographie für viele Anwendungen unpraktisch.

Das zweite Problem, die Nicht-Abstreitbarkeit, besteht darin, dass wir uns oft vergewissern wollen, dass eine bestimmte Nachricht tatsächlich von einem bestimmten Subjekt gesendet wurde. Wenn ein Subjekt eine Nachricht von einem anderen Subjekt erhält und die beiden Subjekte die einzigen sind, die den zur Verschlüsselung verwendeten Schlüssel kennen, ist jedes Subjekt sicher, dass das andere Subjekt der Autor der Nachricht ist. Umgekehrt weiß jedes Subjekt, da nur es den Schlüssel kennt, dass nur das andere Subjekt die Nachricht lesen kann. Das Problem tritt auf, wenn dies gegenüber einem Dritten nachgewiesen werden muss, z. B. bei einem Rechtsstreit, da dieser Mechanismus nicht funktioniert: Jede Partei kann eine Nachricht erstellen, sie verschlüsseln und dann behaupten, dass die andere Partei der Verfasser ist. Das Problem der Nichtabstreitbarkeit wird durch die Verwendung symmetrischer Kryptographie nicht gelöst.

Die für die asymmetrische Kryptografie erforderlichen Berechnungen sind wesentlich komplexer und ressourcenintensiver als die von symmetrischen Algorithmen verwendeten. Um dieses Problem zu überwinden, werden die über ein Netz gesendeten Nachrichten (die in der Regel lang sind) in der Regel mit einem symmetrischen Algorithmus verschlüsselt und der verwendete symmetrische Schlüssel (der kurz ist, einige Hundert Bytes) wird mit einem asymmetrischen Algorithmus verschlüsselt. Auf diese Weise wird die Vertraulichkeit gewährleistet.

Um die Identifizierung des Absenders zu gewährleisten und eine Nichtabstreitbarkeit herzustellen, ist ein Mechanismus zur Zertifizierung der Zuordnung eines öffentlichen Schlüssels zu einem Subjekt erforderlich. Eine Public-Key-Infrastruktur (PKI) bietet Möglichkeiten, um sicher zu sein, dass ein bestimmter öffentlicher Schlüssel mit einer bestimmten Person oder Institution verbunden ist.

Hash-Funktionen. Symmetrische und asymmetrische kryptografische Algorithmen wandeln beide einen Klartext in einen Chiffretext und dann wieder in einen Klartext um. Eine Hash-Funktion ist ein Einweg-Verschlüsselungsalgorithmus: Diese Funktion, die auf einen Klartext angewendet wird, ergibt einen Hash genannten Geheimtext fester Größe (z. B. 256 Byte), aus dem der Klartext nicht wiederhergestellt werden kann. Der Schlüssel zu ihrer Nützlichkeit liegt darin, dass es extrem schwierig ist, einen Klartext mit einem bestimmten Hashwert zu finden. Hash-Algorithmen werden verwendet, um die Integrität von Daten zu gewährleisten, z. B. indem eine Nachricht zusammen mit ihrem eigenen Hash gesendet wird. Beim Empfang der Nachricht sollte derselbe Hash-Algorithmus, der auf den Nachrichtentext angewendet wird, denselben Hash-Wert ergeben, andernfalls wurde die Nachricht während der Übertragung verändert. Aus Sicherheitsgründen kann der Hash-Wert mit dem privaten Schlüssel des Absenders verschlüsselt werden; dies ist die Grundlage des Protokolls der digitalen Signatur.