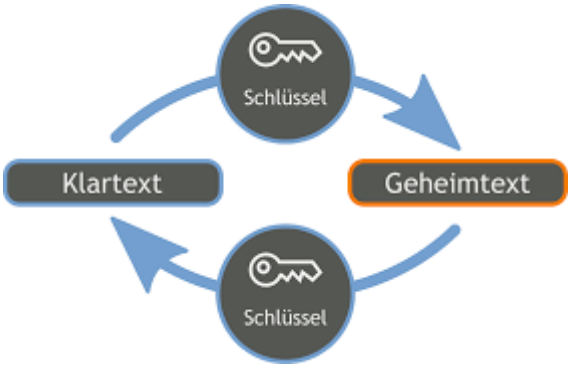
Symmetrische Verschlüsselung (= Secret-Key Verschlüsselung)

Im Gegensatz zum asymmetrischen Verschlüsseln wird beim symmetrischen Verschlüsseln von beiden Kommunikationspartnern derselbe Schlüssel verwendet.



Geschichtliches:

Die symmetrische Verschlüsselung wurde schon vor über 2000 Jahren angewendet, um geheime Botschaften zu übermitteln. Das wohl bekannteste Verfahren ist die Caesar-Verschlüsselung, die nach dem Feldherrn Gaius Julius Caesar benannt wurde. Sie wurde von ihm verwendet, um geheime militärische Nachrichten zu übermitteln

Problem (Schlüsselaustausch)

Weil zum Verschlüsseln derselbe Schlüssel verwendet wird wie zum Entschlüsseln, muss dem Empfänger der Nachricht der Schlüssel schon bekannt sein. Der Sender kann jedoch nicht den Schlüssel gemeinsam mit der Nachricht versenden, da jeder beliebige Benutzer die Nachricht abhören könnte und dadurch die Nachricht mithilfe des Schlüssels entschlüsseln könnte.

Problemlösung des Schlüsselaustausches

Der Schlüsselaustausch ist nur dann sicher, wenn sich die Kommunikationspartner persönlich treffen würden, um den Schlüssel auszutauschen. Eine elegantere Lösung wäre es, wenn der Schlüssel mithilfe einer asymmetrischen Verschlüsselung ausgetauscht wird. Diese Verschlüsselungsart wird dann „Hybride Verschlüsselung“ genannt.

Manuel Repetschnig & Philipp Schuler

Kerckhoffs‘ Prinzip (wird später gebraucht)

Das Kerckhoffs’sche Prinzip oder Kerckhoffs’ Maxime ist ein im Jahr 1883 von *Auguste Kerckhoffs* formulierter Grundsatz der modernen Kryptographie, welcher besagt, dass die Sicherheit eines (symmetrischen) Verschlüsselungsverfahrens auf der Geheimhaltung des Schlüssels beruht anstatt auf der Geheimhaltung des Verschlüsselungsalgorithmus. Dem Kerckhoffs’schen Prinzip wird oft die sogenannte „Security through obscurity“ gegenübergestellt: Sicherheit durch Geheimhaltung des Verschlüsselungsalgorithmus selbst, möglicherweise zusätzlich zur Geheimhaltung des bzw. der verwendeten Schlüssel.

Bekannte Vertreter der symmetrischen Verschlüsselung

Caesar-Verschlüsselung

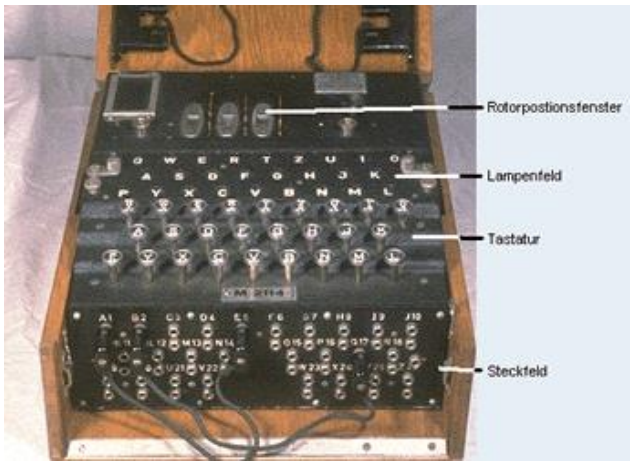
Bsp.: Alice will Bob den Satz „Hallo“ senden, aber Eve soll dies nicht verstehen können. Bei der Caesar-Verschlüsselung wird ein bestimmter Buchstabe um *n* Stellen verschoben, um den Text bzw. die Information unkenntlich zu machen. Zum Entschlüsseln wird der Inhalt um n Stellen in die entgegengesetzte Richtung verschoben

Wenn also der gegebene Satz um Beispielsweise 5 Stellen verschoben wird, ergibt sich daraus das Der Satz *Mfqtt, Bnj limy jx inw?* Beim Alphabet muss man jedoch nur 26 Möglichkeiten durchprobieren, bis man die Nachricht geknackt hat. Wenn man ASCII-Zeichen verwenden würde, würden sich je nach ASCII Tabelle 128 bzw. 256 Mögliche Kombinationen ergeben, diese können dennoch viel zu schnell gelöst werden. Dadurch dass Eve also, wenn sie weiß, dass es sich um die Caesar-Verschlüsselung handelt, den Code knacken könnte, gilt das Kerckhoffs‘ Prinzip nicht.

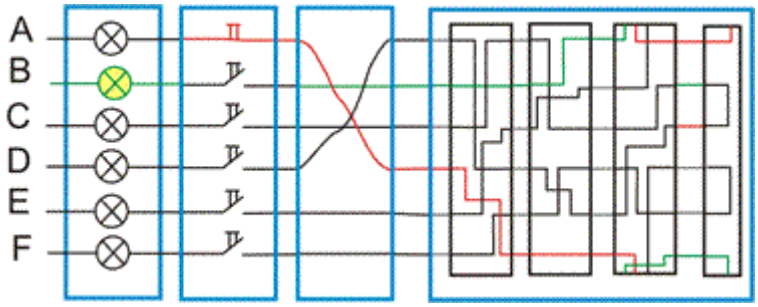
- Vorteile
    - Einfach
    - Schnell
- Nachteile
    - Probleme bei Schlüsselübertragung
    - Kerckhoffs‘ Prinzip gilt nicht
    - Verschlüsselte Inhalte werden mit dem gleichen Vorgangsweise entschlüsselt

Manuel Repetschnig & Philipp Schuler

Enigma-Verschlüsselung



Ist eine Verschlüsselungsmaschine aus dem 2. Weltkrieg. Sie bestand aus einer oder mehreren Walzen, einer Tastatur und verschiedenen Lampen. Wenn man eine Taste auf der Tastatur betätigte, leuchtete der verschlüsselte Buchstabe, welcher zum eingegebenen Buchstaben passte, auf. Das besondere dabei war es, dass sich die Walze bzw. die Walzen innerhalb der Maschine bei jeder Tastenbetätigung drehten, sodass für einen Buchstaben mehrere Ausgänge möglich waren



Als Schlüssel musste die Walzenstellung übergeben werden, um den Code wieder mit einer anderen Enigma-Maschine zu entziffern.

- Vorteile
    - Einfach
    - Schnell
- Nachteile
    - Probleme bei Schlüsselübertragung
    - Kerckhoffs‘ Prinzip gilt nicht

Vignere

Der Eingangstext wird mit einem Vorgegebenen wie bei Caesar verschlüsselt, nur dass die Stellenanzahl nicht immer gleichbleibt.

Manuel Repetschnig & Philipp Schuler

Bsp: Eingangstext: Schule, Schlüssel = 3624

S C H U L E

3 6 2 4 3 6

➔ VIJYOK

AES/DES

Blockverschlüsselung, funktioniert auf binärer Ebene

Genaue Beschreibung und Erklärung im Handout von *Okan Güclü*

Quellen:

Kerckhoffs'sche Prinzip: https://de.wikipedia.org/wiki/Kerckhoffs'_Prinzip

Enigma:
https://www.mathematik.de/spudema/spudema_beitraege/beitraege/hillebrand/mathe2002/enigma.htm

Symmetrische Verschlüsselung(Overview und Geschichtliches):
https://studyflix.de/informatik/symmetrische-verschlusselung-1610