Kryptologie

Marvin Baeumer **2023-12-07 16:16**

Symetrische/Asymetrische Verfahren

> Ein symmetrisches Verschlüsselungsverfahren wird angewendet, wenn derselbe Schlüssel sowohl für die Verschlüsselung als auch für die Entschlüsselung verwendet wird. Beim Caesar, Vigenere- oder One Time Pad Verfahren wird beispielsweise ein gemeinsamer Schlüssel genutzt, um die Chiffre zu entschlüsseln oder den Klartext zu verschlüsseln. Dies setzt voraus, dass sowohl der Sender als auch der Empfänger den Schlüssel kennen. Dazu muss der Schlüssel ausgetauscht werden.

$$\text{Formel fuer Anzahl Schluessel fuer n Teilnehmer}$$

$$\frac{n \cdot (n-1)}{2}$$

> Ein asymmetrisches Verschlüsselungsverfahren, wie das RSA-Verfahren, verwendet hingegen nicht denselben Schlüssel für die Ver- und Entschlüsselung einer Nachricht. Stattdessen werden ein privater und ein öffentlicher Schlüssel verwendet. Der private Schlüssel bleibt geheim, während der öffentliche Schlüssel öffentlich zugänglich ist. Wenn man nun eine Nachricht von Person A an Person B schicken will, muss Person A den öffentlichen Schlüssel von Person B nehmen und damit die Nachricht verschlüsseln. Mit dem Privat Key von Person B kann Person B nun die Nachricht entschlüsseln.

$$\text{Formel fuer Anzahl Schluessel fuer n Teilnehmer}$$

$$2 \cdot n$$

Schlüsselaustauschproblem

> Das Schlüsseltauschproblem in der Kryptologie bezieht sich darauf, wie zwei Parteien sicher einen gemeinsamen geheimen Schlüssel austauschen können. Dies ist entscheidend für sichere Kommunikation. In asymmetrischer Kryptografie müssen die Parteien ihre öffentlichen Schlüssel austauschen, während in symmetrischer Kryptografie der gemeinsame Schlüssel sicher geteilt werden muss. Beispiele für Lösungen sind das Diffie-Hellman-Schlüsselaustauschprotokoll, ein hybrides Verfahren.

Monoalphabetisch und Polyalphabetisch

> Monoalphabetische Verschlüsselungen sind Verfahren, bei denen dieselben Buchstaben gleich verschlüsselt werden. Zum Beispiel wird bei dem Caesar-Verfahren jeder Buchstabe um n Schritte verschoben, wodurch Buchstaben immer gleich verschlüsselt werden. Bei einer polyalphabetischen Verschlüsselung ist dies nicht der Fall. Dort werden gleiche Buchstaben unterschiedlich verschlüsselt, wie zum Beispiel beim Vigenère-Verfahren.

Diffie-Hellmann Verfahren

- Waehlen zweier Zahlen p, g
  - $p \to \mathbb{P}$
  - $g \to \mathbb{N}, g < p$
- Waehlen von $a \in \mathbb{N};\ a < p;\ \ b \in \mathbb{N};\ b < p$
- Berechnung von A, B

$$Formel$$

$$A = g^a \mod p \qquad B = g^b \mod p$$

- Berechnung von K

$$Formel$$

$$K_1 = B^a \mod p \qquad K_2 = A^b \mod p$$

> Das Diffie-Hellman-Verfahren dient dem sicheren Schlüsselaustausch zwischen zwei Parteien. K ist dann der gemeinsame geheime Schlüssel und löst somit das Schlüsselaustauschproblem. Das Diffie-Hellman-Verfahren wird bei symmetrischen Verschlüsselungsverfahren benötigt.

Beispiel

$$p = 31, g = 15$$

Person A	Person B
$a = 25$	$b = 14$
$A = 15^{25} \mod 31$ = 30	$B = 15^{14} \mod 31 = 2$
$K = 2^{25} \mod 31 = 1$	$K = 30^{14} \mod 31 = 1$

Beweis

Unter Anwendung der Potenzgesetze erhält man
$K_1 = B^a \mod p = (g^b \mod p)^a \mod p = (g^{a \cdot b}) \mod p = (g^a \mod p)^b \mod p = A^b \mod p$

- Zuerst betrachtet man die Berechnung von B, dadurch das B mit $g^b \mod p$ berechnet wird kann man für B einsetzen. Somit erhält man $(g^b \mod p)^a \mod p$.
- Daraus folgt nach den Potenzgesetzen $(g^{a \cdot b}) \mod p$, zudem faellt das Innere $\mod p$ weg, weil wir immernoch in der selben Restklasse sind.
- Nun will man in die Form A, weil man beweisen will das $B^a \mod p = A^b \mod p$ ist. A entspricht $g^a \mod p$ deswegen formt man um zu $(g^a \mod p)^b \mod p$ somit kann man dann $(g^a \mod p)^b \mod p$ vereinfachen zu $A^b \mod p$ rechnen.
- Somit ist Bewiesen das $B^a \mod p = A^b \mod p$

Man in the middle Attack

> Bei der "Man-in-the-Middle-Attacke" setzt sich eine Person C zwischen die Kommunikation von Person A und Person B. Die Person C kann sich nun als Person B ausgeben, wenn Person A mit Person B kommunizieren möchte. Es werden insgesamt zwei Diffie-Hellman-Verfahren durchgeführt: einmal zwischen Person A und Person C und einmal zwischen Person B und Person C.

Square and Multiply

$$x^{23} = 22 \text{ Multiplikationen}$$

1. Schritt: 23 in Binaer schreiben (immer die zweier Potenzen nehmen)

$$23 = 1 \cdot 16 + 0 \cdot 8 + 1 \cdot 4 + 1 \cdot 2 + 1 \cdot 1$$

$$10111$$

2. Schritt: Jede 1 wird ersetzt durch QM und jede 0 durch Q - $M \rightarrow Multiplizieren$ - $Q \rightarrow Quadrieren$

$$10111 = QMQQMQMQM$$

3. Schritt: Erstes QM streichen! $\rightarrow$ jede pos Binaer Zahl faengt mit 1 an!

$$10111 = QQMQMQM$$

$$(((((x^2)^2) \cdot x)^2) \cdot x)^2 \cdot x$$

$$((x^4 \cdot x)^2 \cdot x)^2 \cdot x = (x^{10} \cdot x)^2 \cdot x = x^{22} \cdot x = x^{23}$$

> 7 Multiplikationen statt 22!

Die drei Schutzziele der Kryptologie

- Vertraulichkeit: Der Inhalt einer Nachricht ist nur für einen bestimmten Empfängerkreis verfügbar.
- Integrität: Der Inhalt einer Nachricht kann nicht unbemerkt verändert werden.
- Verbindlichkeit: Der Sender einer Nachricht kann nicht abstreiten, diese versendet zu haben

Caesar Verfahren

> Bei dem Caesar Verfahren wird das Alphabet zum Verschluesseln um n Schritte nach rechts verschoben und zum Entschluesseln nach n Schritte nach links.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**

Klartext	**H**	**A**	**L**	**L**	**O**	**n = 3**
Ciphertext	K	D	O	O	R	n = 3

Vigenere Verfahren

> Das Vigenere Verfahren verschlüsselt mithilfe eines Wortes als Schlüssel. Dazu gibt es eine Tabelle, die die alphabetische Verschiebung darstellt. Man geht in der oberen Zeile für den Buchstaben x des Klartextes und geht dann nach unten, solange bis rechts der Buchstabe x des Schlüssels steht.

	A	**B**	**C**	**D**	**E**	**F**	**G**	*H*	**I**	**J**	**K**	**L**
A	A	B	C	D	E	F	G	H	I	J	K	L
B	B	C	D	E	F	G	H	I	J	K	L	M
C	C	D	E	F	G	H	I	J	K	L	M	N
D	D	E	F	G	H	I	J	K	L	M	N	O
E	E	F	G	H	I	J	K	L	M	N	O	P
F	F	G	H	I	J	K	L	M	N	O	P	Q
G	G	H	I	J	K	L	M	N	O	P	Q	R
H	H	I	J	K	L	M	N	O	P	Q	R	S
I	I	J	K	L	M	N	O	*P*	Q	R	S	T
J	J	K	L	M	N	O	P	Q	R	S	T	U
K	K	L	M	N	O	P	Q	R	S	T	U	V
L	L	M	N	O	P	Q	R	S	T	U	V	W
M	M	N	O	P	Q	R	S	T	U	V	W	X
N	N	O	P	Q	R	S	T	U	V	W	X	Y
O	O	P	Q	R	S	T	U	V	W	X	Y	Z
P	P	Q	R	S	T	U	V	W	X	Y	Z	A
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B
R	R	S	T	U	V	W	X	Y	Z	A	B	C
S	S	T	U	V	W	X	Y	Z	A	B	C	D
T	T	U	V	W	X	Y	Z	A	B	C	D	E
U	U	V	W	X	Y	Z	A	B	C	D	E	F
V	V	W	X	Y	Z	A	B	C	D	E	F	G
W	W	X	Y	Z	A	B	C	D	E	F	G	H
X	X	Y	Z	A	B	C	D	E	F	G	H	I
Y	Y	Z	A	B	C	D	E	F	G	H	I	J
Z	Z	A	B	C	D	E	F	G	H	I	J	K

Klartext	*H*	*A*	*L*	*L*	*O*	**n = IST**
Schluessel	*I*	*S*	*T*	*I*	*T*	n = IST
Ciphertext	*P*	*S*	*E*	*T*	*G*	n = IST
### [[Zahlentheorie#RSA-Verfahren	RSA Verfahren]]					