Modul V3 – Öffentliche Schlüsselkonstruktion

Zeitrahmen
30 - 40 Minuten (je nach Tiefe der Nachbesprechung

Zielgruppe
Sekundarstufe II

Inhaltliche Voraussetzungen
- Lehreinheit V2 Symmetrische Schlüssel
- Taschenrechner/Computer zur Berechnung der Werte bei der Ver- und Entschlüsselung

Lehrziel
Problem der Schlüsselverteilung bei der symmetrischen Verschlüsselung verstehen.
Verstehen des Prinzips und Vorteils der Nutzung asymmetrischer Verschlüsselung.

Motivation
Geheime Nachrichten wecken die Neugierde. Kryptografie ist ein zentrales Thema der Mathematik/ Informatik. Sie war historisch gesehen schon früh von Bedeutung und wird in der heutigen virtuellen Kommunikation noch immer wichtiger. Nicht jedes Verschlüsselungsverfahren ist bei jedem Anwendungsgebiet sicher. Einfache symmetrische Verschlüsslungsverfahren haben den Nachteil, dass sie von der Vertraulichkeit der Schlüsselübertragung abhängen. Diese Begrenzung wollen wir nun überwinden.

Requisiten
- Einfache ASCII Tabelle (siehe Rückseite der Arbeitsblätter)
- Verzeichnis für öffentliche Schlüssel; Blatt Papier wo dieser notiert wird genügt

Unterlagen
V-AB 3.1, V-AB 3.2, V-AB 3.3

Partizipanden
Gesamte Klasse, teilweise in Gruppen unterteilt

Vorgehensweise
1. Um das System der Verschlüsselung ohne Schlüsselübergabe zu realisieren beschäftigt man sich mit *mathematischen Funktionen*. Alle Formen der computergestützten Verschlüsselung kann man als Funktion betrachten, die eine Zahl/Nachricht (den Klartext) in einen andere (den Geheimtext) verwandelt.

   Welche einfachen Beispiele für Funktionen finden wir in der Mathematik/ oder im Alltag (nicht zu kompliziert denken!)?

   - *Das Verdoppeln einer Zahl ist eine einfache Funktion. Dabei wird beispielsweise 6 aus 3 oder 18 aus 9. Kehrt man die Funktion um erhält man wieder den Ursprungswert.*
   - *Einen Lichtschalter könnte man auch als Funktion ansehen. Man schaltet das Licht ein, und die Funktion ist umkehrbar, da man das Licht auch wieder ausschalten kann, womit der ursprüngliche Zustand wieder entsteht.*

Solche Funktionen nennt man *umkehrbar*. Eine nicht umkehrbare Funktion wäre etwa x^2, da die Wurzel aus x^2 sowohl x als auch –x sein könnte. Die Funktion x^2 ist also nicht umkehrbar.
Für die Kryptografie war es wichtig, nicht umkehrbare Funktionen zu finden die durch Zusatzinformation allerdings umkehrbar gemacht werden können. Man nennt diese auch *Einwegfunktionen* oder Einwegfunktionen mit Falltüre, da durch die Zusatzinformation (Falltüre) die Funktion umkehrbar wird.

Mit welchen alltäglichen Handlungen könnte man Einwegfunktionen vergleichen?

- *Das Mischen von zwei Farben ist eine Einwegfunktion: Es ist leicht die Farben grün und gelb zu mischen, allerdings ist es sehr schwierig, dieses Gemisch wieder zu trennen oder herauszufinden, wie viele Teile von welcher Farbe genommen wurden.*
- *Auch das Zerschlagen eines Eies könnte eine Einwegfunktion sein. Das Ei kann nicht mehr in den ursprünglichen Zustand gebracht werden.*
- *Bei einer Addition zweier Zahlen z. B.: a + b = 20 ergeben sich viele Möglichkeiten, woraus das Ergebnis 20 entstanden sein kann. Man kann allenfalls probieren und raten.*
- *Ist allerdings bekannt, dass a = 17 sein soll, also 20 die Summe aus 17 + unbekannt ist, lässt sich „unbekannt" leicht errechnen. – Erinnert euch an die Konstruktion von Vigenère-Verschlüsselung von binär codierten Folgen.*
- *Ein weiteres Beispiel für eine Einwegfunktion wäre die Funktion y^x mod P. Dadurch, dass y zur x-ten Potenz erhoben wird, entsteht eine sehr große Zahl. Durch die Restbildung (mod P) wird diese nochmals „durchmischt" und auf eine erträgliche Größe gekürzt.*

2. ***Arbeitsblätter Schlüsselvereinbarung:*** Nun wird die Klasse in 3 etwa gleich große Gruppen geteilt. Es soll gezeigt werden, dass ein Schlüssel vereinbart werden kann, ohne dass sich die beiden Partner treffen, daher wird angenommen, dass die Kommunikation zwischen den beiden Gruppen telefonisch erfolgt.

Die Teilnehmer erhalten am Arbeitsblatt Hilfestellungen und Teillösungen. Daher sollten die Arbeitsblätter auch unbedingt verwendet werden.

Gruppe A und B: diese beiden Gruppen möchten geheime Nachrichten miteinander austauschen. Siehe Arbeitsblatt V-AB3.1 und V-AB3.2
Gruppe C: diese Gruppe möchte die Nachrichten zwischen A und B abhören, sie hat die Telefonleitung angezapft. Siehe V-AB3.3

a. Die drei Gruppen bekommen den Arbeitsauftrag und die Arbeitsblätter V_AB3.1 bis V-AB3.3.

b. Gemeinsame Vorbereitung: Es wird die Einwegfunktion **Y^x mod P** verwendet. Dies muss allen drei Gruppen bekannt sein.

Exponentiation wird als bekannt vorausgesetzt. Die Notation Y^x, also scheinbar eine unbekannte im Exponenten könnte jedoch für Erstaunen sorgen, auch wenn sich später zeigt, dass dieses X nicht als Unbekannte sondern als Variable zu verstehen ist. Wir erklären dennoch kurz:

Ihr kennt die Exponentiation, also z.B. $Y^2 = Y * Y$, dementsprechend ist $Y^3 = Y * Y * Y$ und so weiter für jeden beliebigen, ganzzahligen Exponenten. Daher ist auch $Y^X = Y * Y * \ldots * Y$, insgesamt X-mal.

Eventuell muss an dieser Stelle allerdings die Modulo-Operation erläutert werden:

Beginnen wir zum Beispiel mit dem Produkt zweier Zahlen. Hier nehmen wir der Einfachheit halber zwei kleine Primzahlen, etwa 11 * 9 = 99.
Die Modulo-Operation liefert uns den Rest nach Division durch den 2. Operanden dieser Funktion. Also wegen

99 / 13 = 7, Rest 8

ist

99 mod 13 = 8 oder allgemein, für Z mod q = r der Rest r stets zwischen 0 und (q-1).

Wir können jede Zahl als die Summe aus dem Produkt zweier Zahlen mit dem Rest, also aus

$$z = n*q + r = n*q + z \bmod q$$

darstellen.
Ab hier unterscheiden sich die Aufgaben für die 3 Gruppen. Daher wird in der folgenden Tabelle der Ablauf parallel dargestellt.

Gruppe A	Gruppe B	Gruppe C
Die Gruppen A und B vereinbaren untereinander die Werte für Y, die Basis, und P, den Quotient zur Modulo-Berechnung. Diese Werte können auch von Gruppe C mitgehört werden. Y muss kleiner als P sein! (Beispielsweise Y=7, P=11, 7^x mod 11) Die Werte werden per „Telefon“ (hier durch Zuruf) vereinbart. Die Gruppe C kann mithören.	Die Gruppen A und B vereinbaren untereinander die Werte für Y, die Basis, und P, den Quotient zur Modulo-Berechnung. Diese Werte können auch von Gruppe C mitgehört werden. Y muss kleiner als P sein! (Beispielsweise Y=7, P=11, 7^x mod 11) Die Werte werden per „Telefon“ (hier durch Zuruf) vereinbart. Die Gruppe C kann mithören.	Gruppe C notiert sich, was sie mithört, also die Werte für Y und P.
Eine geheime Zahl A wird von Gruppe A ausgewählt und in die Einwegfunktion Y^x mod P für X eingesetzt, sowie das Ergebnis $\alpha=Y^A$ mod P berechnet. Das Ergebnis α kann nun an die andere Gruppe (an Gruppe B) übertragen werden.	Eine geheime Zahl B wird von Gruppe B ausgewählt und in die Einwegfunktion Y^x mod P für X eingesetzt, sowie das Ergebnis $\beta=Y^B$ mod P berechnet. Das Ergebnis β kann nun an die andere Gruppe (an Gruppe A) übertragen werden.	
Der Wert α wird nun an die Gruppe B „telefonisch“ (also wieder durch Zurufen) unverschlüsselt übertragen.	Der Wert β wird nun an die Gruppe A „telefonisch“ (also wieder durch Zurufen) unverschlüsselt übertragen.	Gruppe C notiert sich wieder alle Werte die mitgehört werden, also α und β.
Nun wird der Wert β, der von Gruppe B übermittelt wurde, verwendet und als Basis Y in die Einwegfunktion eingesetzt. Ebenso wird der in der Gruppe für A bestimmte Wert als Exponent eingesetzt und so nochmals die Einwegfunktion berechnet.	Nun wird der Wert α, der von Gruppe A übermittelt wurde verwendet und als Basis Y in die Einwegfunktion eingesetzt. Ebenso wird der in der Gruppe für B bestimmte Wert als Exponent eingesetzt und so nochmals die Einwegfunktion berechnet.	Gruppe C hat nun 4 Werte mitgehört. Die Aufgabe dieser Gruppe ist es, den vereinbarten Schlüssel daraus zu berechnen. Es fehlen dafür aber die geheimen Werte A und B aus den beiden gleichnamigen Gruppen.

$S_A = \beta^A \bmod P.$	$S_B = \alpha^B \bmod P.$	
Das Ergebnis dieser Berechnung ist der soeben vereinbarte gemeinsame Schlüssel S, da $S_A = S_B$.	Das Ergebnis dieser Berechnung ist der soeben vereinbarte gemeinsame Schlüssel S, da $S_A = S_B$.	

Und hier die Ergebnisse der obigen Rechenaufgaben, passend zu den Zahlen auf den Arbeitsblättern V-AB3.1 bis V-AB 3.3

Ergebnisse des Beispiels für Y=7, P=11 und A=3, B= 6:
α= 2, β= 4 und S = 9.

Die Gruppen A und B haben sich nun nach diesem von Whitfield Diffie und Martin Hellman 1976 vorgeschlagenen Verfahren der öffentlichen Schlüsselkonstruktion einen Schlüssel vereinbart, der ihr gemeinsames Geheimnis darstellt. So wie in Einheit E-V 2 – Verschlüsselung mit symmetrischen Schlüsseln gezeigt, kann binär codierte Information nun mit dem in diesem Verfahren vereinbarten, nach wie vor symmetrischen Schlüssel S verschlüsselt werden.
Allerdings erinnern wir uns, dass die Qualität dieser Verschlüsselung stark von der Schlüssellänge abhängt. In der Praxis wird man daher nicht einen so kurzen Schlüssel verwenden, wie wir in eben berechnet haben. Da die Dauer der Berechnung des Schlüssels relativ zur Häufigkeit der Verwendung des Schlüssels keine Rolle spielt, darf schon einiger Aufwand in die Berechnung von S gesteckt werden.

Mit Hilfe von Arbeitsblatt V-AB 3.4 verschlüsseln wir nun einen ganz kurzen Text, oder auch nur einen Buchstaben. Wir erkennen dabei, dass ein einstelliger dezimaler (dreistelliger binärer) Schlüssel noch wenig Sinn ergibt. Man kann sich jedoch leicht vorstellen, dass bei hinreichend großem P (und entsprechendem Y, A und B) sehr lange Schlüssel entstehen.

Eine Regel lautet, dass sich die Länge eines binären Schlüssels nicht durch 8 teilen lassen sollte (in unserem Fall sollte sie sich nicht durch 7 teilen lassen). Warum wohl?
Hinweis: Macht einen Blick auf die vereinfachte ASCII-Tabelle in V-AB 3.4!

Erweiterter ASCII-Code hat 8 Bit (unser vereinfachter nur 7 Bit). Wenn die Grenze des Schlüsselwortes mit der Grenze der Codierung einzelner Buchstaben zusammenfällt, wird das Decodieren ungleich leichter, als wenn dies nicht der Fall ist und gleiche Buchstaben je nach Position im Text unterschiedlich verschlüsselt werden.

Nehmen wir an, wir hätten einen hinreichend langen Schlüssel, dessen Schlüssellänge keine Gemeinsamkeit mit der Wortlänge in der Codierungstabelle hat. Gegen welche Attacke ist dieses Verfahren nicht gefeit?

Diese Frage ist wohl etwas schwierig, da sie von einer völlig anderen Bedrohung ausgeht als bisher angenommen. Es geht um „Enemy in the Loop"-Attacken. Hier gibt sich der Angreifer als Empfänger der Nachricht aus und führt an Stelle des richtigen Empfängers den Schlüsseltausch aus. Wenn er dies sowohl mit Sender wie beabsichtigtem Empfänger macht, glauben beide, sie würden verschlüsselt kommunizieren. Tatsächlich entschlüsselt der Lauscher in der Mitte und verschlüsselt anschließend mit seinem Schlüssel.

Nachbesprechung

Der zweite Teil dieser Nachbesprechung ist insbesondere für Schülerinnen und Schüler gedacht, die nicht gerne an Zauberei glauben und über ein gewisses mathematisches Interesse verfügen. Um diesen Teil zu verstehen, benötigt man lediglich die ohnehin bekannten Exponentiationsregeln und die eingangs der Einheit vorgestellte Modulo-Funktion.

Gruppe A und B haben den Schlüssel nie direkt miteinander ausgetauscht, aber trotzdem den gleichen Schlüssel erhalten. Sie können den Schlüssel nun offenlegen. C war es nicht möglich aus den mitgehörten Informationen auf den vereinbarten Wert zu schließen, da es sich bei Y^X mod P um eine Einwegfunktion handelt.
Vergleicht man das Vorgehen wieder mit dem Mischen von Farben und nimmt man an, dass alle Beteiligten einen Liter gelber Farbe haben, und A und B mit diesen Farben einen Geheimschlüssel erstellen wollen. A und B wählen jeder für sich einen Liter frei gewählter Farbe und mischt diesen zur gelben Farbe. A nimmt also z.B. einen Liter roter Farbe, B einen Liter grüner Farbe. A schickt den Farbkanister mit der gemischten Farbe an B und B schickt den Farbkanister mit der von ihm gemischten Farbe an A. A und B wissen gegenseitig nicht, welche Farbe die andere Gruppe gewählt hat, genauso wenig wie C weiß welche Farbe diese gewählt haben. Kommt der Kanister an, mischen A und B jeweils ihre eigenen Farben zum Gemisch dazu. Beide erhalten dadurch dieselbe Farbe, den vereinbarten Schlüssel. C kann allerdings die Farbe nicht rekonstruieren.

Nach dieser ausführlichen Erklärung mit den Farben sollte noch das Geheimnis gelüftet werden, warum Gruppe A und B denselben Schlüssel erhielten. Die beiden Gruppen legen nun ihre „privaten“ geheimen Exponenten offen: A=3 und B=6.
Daraus können wir α und β berechnen. Gruppe C kann nun nachprüfen, ob nicht geschwindelt wurde. Gemeinsam sollten wir nun versuchen, zu Erfahren, wie die Farbanalyse mit den Zahlen funktioniert.

Für Gruppe A:
$S = \beta^A \bmod 11$ und
wegen $\beta = 7^6 \bmod 11$
$S = (7^6 \bmod 12)^3 \bmod 11$

Für Gruppe B:
$S = \alpha^B \bmod 11$ und
wegen $\alpha = 7^3 \bmod 11$
$S = (7^3 \bmod 11)^6 \bmod 11$

Wir erkennen bereits, dass das Produkt der Exponenten gleich ist 6*3 = 3*6, also wäre $7^{6*3} \bmod 11$ gleich
$7^{3*6} \bmod 11$. Allerdings müssen wir noch prüfen, ob die zur Berechnung von α und β vorgenommene Modulo-Bildung diese Gleichheit nicht zerstören könnte. Hier erinnern wir uns daran, dass Y < P sein musste, oder in unserem Fall 7 < 11 gegolten hat.

Bleiben wir beim konkreten Beispiel und berechnen wir

x	Y^X	7^x	$7^x \bmod 11$	$7^x = n*g + Rest = n*P + Rest$	$(7^{x-1} \bmod P) * 7$	$(7^{x-1} \bmod P)*7 \bmod P$
1	7	7	7	7	1*7 = 7	7
2	7*7	49	5	44+5 = 4*11 + 5	7*7 = 49	5
3	7*7*7	343	2	341+2 = 31*11 + 2	5*7 = 35	2
4	…	1401	3	2398 + 3 = 218*11 + 3	2*7 = 14	3
5	…	16807	10	16797 + 10 = 1527*11 + 10	3*7 = 21	10
6	…	117649	4	117645 + 4 = 10695*11 + 4	10*7 = 70	4

…						…
18						

Wir erkennen aus Spalte 4, dass das Produkt n*q in unserem Fall n*P immer ein Produkt aus P, also in unserem Fall ein Vielfaches von11 ist und daher ohne Rest durch P (11) geteilt werden kann. Jede Zeile hat somit einen Wert der Form $n*P + Y^X \bmod P$.
Die nächste Zeile gewinnen wir entsprechend $Y^{X+1} = Y^X * Y$ (Spalte 2) nun mit der Formel

$$(n*P + Y^X \bmod P) * Y = n*P*Y + (Y^X \bmod P) * Y.$$

Berechnen wir daraus den Rest (die Modulo-Funktion), so erhalten wir

$$Y^{X+1} \bmod P = (n*P*Y) \bmod P + (Y^X \bmod P)*Y \bmod P.$$

Hier wird die 1. Summe, $(n*P*Y) \bmod P$ stets 0 sein, da P ja sowohl Faktor als Divisor ist. Es genügt also eigentlich nur den Rest, also $(Y^X \bmod P) *Y \bmod P$ zu berechnen. Diese Rechnung führen wir schrittweise in Spalte 6 aus und erkennen, dass Spalte 7 identische Werte wie Spalte 3 enthalten muss.
Wir können leicht erkennen, dass dies nicht nur für $(Y^{x-1} \bmod P) * Y \bmod P$ gilt sondern für jeden beliebigen Wert k mit $(Y^{x-k} \bmod P) * Y^k \bmod P$.

Mit diesen Überlegungen sehen wir allerdings auch, dass

$$\alpha^x \bmod P = (Y^A \bmod P)^B \bmod P$$

zu einer ähnlichen Faktorisierung führt.

Setzen wir für α = n*P*Y + Rest, erhalten wir z.B. für B=2 die quadratische Form

$$((n*P*Y+Rest)*(n*P*Y+Rest)) \bmod P, \text{ also}$$

$$((n*P*Y)^2 + 2*n*P*Y + Rest^2) \bmod P.$$

Hierbei ist P in jedem Glied außer Im $Rest^2$ ein Faktor. Somit gilt

$$((n*P*Y)^2 + 2*n*P*Y + Rest^2) \bmod P = Rest^2 \bmod P.$$

Analoges gilt es für jedes Polynom höheren Grades, das durch ausmultiplizieren von $(n*P*Y+Rest)^X$ mod P entsteht. Wir erkennen mithin, dass die Modulo-Operation die Eingangs aufgestellte Überlegungen nicht stört. Wir haben daher

$$(Y^A)^B = Y^{A*B} = Y^{B*A} = (Y^B)^A$$
$$(Y^A)^B \bmod P = (Y^B)^A \bmod P$$
$$(Y^A \bmod P)^B \bmod P = (Y^B \bmod P)^A \bmod P$$

und somit ist geklärt, dass die Modulo-Operation die Symmetrie (*Kommutativität*) der Exponentiation nicht stört und der mathematische Apparat tatsächlich genau so funktioniert wie das Beispiel mit den hintereinander beigemischten Farben.

Quellen:

http://www.netplanet.org/kryptografie/verfahren.shtml (14. 1. 2009)

http://www.gnupp.de/verschluesselung/index.html, (14. 1. 2009)

http://einklich.net/etc/vigenere.htm, (14. 1. 2009)

Hromkovič, Juraj: Sieben Wunder der Informatik. Eine Reise an die Grenze des Machbaren mit Aufgaben und Lösungen. Wiesbaden: Teubner, 2006.

Schaumüller-Bichl Ingrid: Sicherheits-Management: Risikobewältigung in Informationstechnoligischen Systemen; B.I. Wissenschaftsverleg, Mannheim, 1992.

Schulz, Ralph-Hardo: Codierungstheorie. Eine Einführung. Wiesbaden: Vieweg Verlag, 2003.

Singh, Simon: Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet. München: dtv, 2004.