

## V-AB 3.2 Arbeitsblatt zu Modul V3 Schlüsselvereinbarung

Gruppe B



### Aufgabenstellung:

Ihr möchtet mit Gruppe A eine geheime Nachricht austauschen. Allerdings versucht Gruppe C euch zu belauschen. Daher müsst ihr eure Nachricht verschlüsseln.

Da nun aber kein persönliches Treffen zum Schlüsselaustausch für die Verschlüsselung möglich ist, müsst ihr einen anderen Weg wählen. Ihr tauscht die Schlüssel telefonisch aus, aber Achtung (!) C hört auch die Telefonate mit!

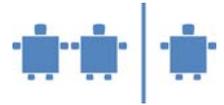
### Vorgehen:

1. Es wird die folgende Einwegfunktion zur Vereinbarung verwendet:  $Y^x \pmod{P}$   
Diese Einwegfunktion ist nicht nur euch bekannt, sondern auch der Gruppe A und euren Gegnern C. Sie ist also öffentlich.
2. Ihr einigt euch nun mit der Gruppe A auf die Werte für Y und P in der Formel. Diese beiden Werte könnt ihr einfach auf einem Zettel oder durch ein Gespräch austauschen. Die Gruppe C darf mitlesen bzw. hören.  $Y=7$ ,  $P=11$ , also entsteht:  $7^x \pmod{11}$
3. Wählt nun eine Zahl B, z.B.  $B=6$  aus, und haltet sie geheim. Setzt diese Zahl für X in die Einwegfunktion ein und berechnet das Ergebnis. Es entsteht also  $\beta = 7^6 \pmod{11} = \underline{\hspace{2cm}}$
4. Nennt nun das Ergebnis eurer Berechnung, also  $\beta$ , der Gruppe A. Dies ist nun die eigentliche Schlüsselvereinbarung. Gruppe C kann wiederum mithören, da sie ja nur  $\beta$  kennt nicht aber B.
5. Gruppe A hat auch Schritt 4 durchgeführt und gibt euch nun ihren Wert. Diesen nennen wir  $\alpha$ .
6. Nehmt also  $\alpha$  und setzt es in eure vereinbarte Formel  $S = \alpha^B \pmod{P}$  ein. Das Ergebnis ist nun euer vereinbarter Schlüssel S!

Schlüssel=       

### Zur Wiederholung:

Öffentlich sind die Werte: Y, P,  $\alpha$ ,  $\beta$



Geheim sind nur die Werte: A, gewählt durch Gruppe A und B, gewählt durch Gruppe B

### V-AB 3.4 – Vereinfachte ASCII-Tabelle

**ASCII-Tabelle für Großbuchstaben:**

|   | Binär   | Dezimal |   | Binär   | Dezimal |
|---|---------|---------|---|---------|---------|
| A | 1000001 | 65      | N | 1001110 | 78      |
| B | 1000010 | 66      | O | 1001111 | 79      |
| C | 1000011 | 67      | P | 1010000 | 80      |
| D | 1000100 | 68      | Q | 1010001 | 81      |
| E | 1000101 | 69      | R | 1010010 | 82      |
| F | 1000110 | 70      | S | 1010011 | 83      |
| G | 1000111 | 71      | T | 1010100 | 84      |
| H | 1001000 | 72      | U | 1010101 | 85      |
| I | 1001001 | 73      | V | 1010110 | 86      |
| J | 1001010 | 74      | W | 1010111 | 87      |
| K | 1001011 | 75      | X | 1011000 | 88      |
| L | 1001100 | 76      | Y | 1011001 | 89      |
| M | 1001101 | 77      | Z | 1011010 | 90      |

Kurzer Text: \_\_\_\_\_

dieser Text dezimal: \_\_\_\_\_

Schlüssel (wiederholt): \_\_\_\_\_

verschlüsselte Ziffernfolge \_\_\_\_\_

verschlüsselter Text \_\_\_\_\_

Kurzer Text: \_\_\_\_\_

dieser Text binär: \_\_\_\_\_

binärer Schlüssel (wdhlt): \_\_\_\_\_

verschlüsselte Bitfolge \_\_\_\_\_

verschlüsselter Text \_\_\_\_\_