V-AB 3.3 Arbeitsblatt zu Modul V3 Schlüsselvereinbarung

Gruppe C

Aufgabenstellung:
Gruppe A und B möchten eine geheime Nachricht austauschen. Dafür müssen sie zuerst den Schlüssel vereinbaren.
Eure Aufgabe ist es, diesen Schlüssel herauszufinden, damit ihr später übertragene Nachrichten entschlüsseln könnt.

Vorgehen:

1. Euch ist bekannt, dass A und B die folgende Funktion verwenden, um den Schlüssel zu vereinbaren: $Y^x \pmod P$

2. Notiert euch die Werte für Y und P die von den beiden vereinbart werden.
   Y= _____
   P= _____

3. Weitere zwei Werte könnt ihr in Erfahrung bringen. Sie ist das Ergebnis der Funktionen der jeweiligen Gruppen. Notiert sie euch.
   α= _____
   β= _____

4. Könnt ihr nun aus diesem Wissen den Schlüssel, den die beiden vereinbart haben rekonstruieren? Folgende Informationen besitzt ihr:
   $\alpha = Y^x \pmod P$
   $\beta = Y^x \pmod P$
   Wie lauteten die beiden Werte für X?

Zur Wiederholung:
Öffentlich sind die Werte: Y, P, α, β
Geheim sind nur die Werte: A, gewählt durch Gruppe A und B, gewählt durch Gruppe B (also die Werte für X)

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 _____ _____ _____ _____ _____ _____ _____