Schlüsselaustausch

Der Diffie-Hellman-Merkle Schlüsselaustausch:

Beide Partner vereinbaren eine Primzahl p und eine Primitivwurzel $[g]$ für $\mathbb{Z}_p$.

Andy wählt $a \in \{1, 2, \ldots, p-2\}$ und berechnet: $A \equiv g^a \mod p$
Berenice wählt $b \in \{1, 2, \ldots, p-2\}$ und berechnet: $B \equiv g^b \mod p$

Dann tauschen Sie A und B aus. Das bedeutet: (p, g, A, B) sind öffentlich bekannt,
a kennt nur Andy,
b kennt nur Berenice.

Jeder von beiden berechnet nun den gemeinsamen Schlüssel K:

Andy berechnet mit seiner Geheimzahl a: $K \equiv B^a \mod p$,
Berenice berechnet mit ihrer Geheimzahl b: $K \equiv A^b \mod p$.

Hinweis: A, B, K müssen zwischen 1 und $p-1$ liegen.

Beide erhalten das selbe K, denn: $B^a \equiv (g^b)^a = g^{ab} = (g^a)^b \equiv A^b \mod p$.

Aufgabe 4

Andy und Berenice vereinbaren $p = 7$ und $g = 3$.

Andy wählt: $a = 3$, berechnet A: $g^a =$ $\mod 7 \Rightarrow A =$

Berenice wählt: $b = 4$, berechnet B: $g^b =$ $\mod 7 \Rightarrow B =$

Hinweis: A, B müssen zwischen 1 und 6 liegen.

Öffentlich bekannt sind also:

$p = 7$, $g = 3$, $A =$, $B =$.

Andy berechnet: $B^a =$ $\mod 7 \Rightarrow K =$

Berenice berechnet: $A^b =$ $\mod 7 \Rightarrow K =$

Hinweis: K muss zwischen 1 und 6 liegen.

Für Andy und Berenice kommt die selbe Zahl K als Ergebnis heraus. Schreibe diese Zahl mit Buchstaben als Wort und verwende dieses Zahlwort als Schlüsselwort für die Vigenère-Entschlüsselung, um die Nachricht auf der Rückseite zu entschlüsseln.

Verschlüsselt	i	z	q	t	i	m	e	w
Schlüssel								
Nachricht								

Aufgabe 5

Andy und Berenice vereinbaren $p = 11$ und $g = 2$. Andy schickt an Berenice die Zahl $A = 5$, Berenice meldet $B = 8$. Kurze Zeit später übermittelt Andy die Nachricht

h i x y z q w k n c t v m

Bestimme a, b und den Schlüssel K, entschlüssle die Nachricht mit dem Zahlwort zu K als Schlüsselwort für Vigenère-Entschlüsselung.

Hinweis: Verwende die Tabelle der Potenzen $[2]^k$ aus Aufgabe 3b (Arbeitsblatt 6.3).

Anmerkung: Die Verschlüsselung kann hier geknackt werden, da für p, g, a, b kleine Zahlen verwendet wurden. In der richtigen Anwendung werden sehr große Zahlen verwendet. Dann ist es schwierig, aus g und A die Zahl a zu berechnen.

Vigenère-Quadrat:

Klartext→	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Schlüsselwort	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	k
	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	l	l	m	n	o
	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y