Kryptologie, SS03 Aufgabenblatt 5

Zur Lösung der folgenden Aufgaben sollten Sie das Computeralgebrasystem Pari-GP verwenden (www.parigp-home.de) . Bei der Darstellung der Lösungen sind die benutzten Pari Inputs und Outputs genau zu dokumentieren.
Alle zur Nutzung des Programms notwendigen Informationen sind der dem Programmpaket beiliegenden Pari-Reference Card und ggf. dem User's Guide zu entnehmen.

Aufgabe 1 (Diffie-Hellman in $\mathbb{Z}_p^*$)

p=214834852766454603179122427035869109835564466049396220490607628489081625108575043151
ist eine Primzahl.

a) Finden Sie mittels des Pari-Befehls *factorint* eine Primzahlzerlegung von $p-1$.
b) Zeigen Sie: 7 ist ein Erzeuger von $\mathbb{Z}_p^*$, 2 dagegen nicht

Benutzen Sie im folgenden das Diffie-Hellman System mit der Gruppe $\mathbb{Z}_p^*$ und dem Erzeuger 7.

A habe den geheimen Schlüssel
a = 14091823657179212627803243834235168922805366857335984715812693090921373653905881 1972
und den zugehörigen öffentlichen Schlüssel $K_{\text{Pub}}(A) = 7^a =$
118295899503098080709004859618151590978127387993567221838083523595039752396157705117

B möchte mit A kommunizieren, erzeugt die Zufallszahl k=
208584777037225408454971444316535562052632813807153879553328394666236700163348444294 ,
den Mailheader $MH = 7^k =$
608393080580766929642700139010836334940566534433701583269031513154766439034643319 01,
sowie den Kommunikationsschlüssel $Sessionkey = K_{Pub}(A)^k =$
810566272413732014954102958693666532845580521483245906905465124907101921796510753 63

c) Zeigen Sie, daß und wie A aus dem Mailheader und seinem geheimen Schlüssel den Kommunikationsschlüssel rekonstronstruieren kann.

Endliche Körper

Das Polynom $f(X) = X^{256} + X^{10} + X^5 + X^2 + 1 \in \mathbb{Z}_2[X]$ ist irreduzibel.
(Es wurde gefunden durch den Pari-Befehl *ffinit*(2,256))

Sind *g*,*h* Polynome von kleinerem Grad und $k \in \mathbb{N}$, so kann man in Pari mit Ausdrücken wie Mod(*g*,*f*)+Mod(*h*,*f*), Mod(*g*,*f*)*Mod(*h*,*f*) und Mod(*g*,*f*)^*k*, und daher in dem endlichen Körper $K = \mathbb{Z}_2[X] / (f)$, welcher 2^{256} Elemente besitzt, rechnen.
In der Pari-Notation ist
f = Mod(Mod(1, 2), Mod(1, 2)*x^256 + Mod(1, 2)*x^10 + Mod(1, 2)*x^5 + Mod(1, 2)*x^2 + Mod(1, 2))

Für jedes Element $a \in K^* = K - \{0\}$ muß aus gruppentheoretischen Gründen offenbar gelten: $X^{2^{256}-1} = 1$. Tatsächlich berechnet Pari auf den Input Mod(x,f)^(2^256-1) das Ergebnis Mod(Mod(1, 2), Mod(1, 2)*x^256 + Mod(1, 2)*x^10 + Mod(1, 2)*x^5 + Mod(1, 2)*x^2 + Mod(1, 2)).

Man kann nun analog zu Aufgabe 1 die Primfaktorzerlegung von $|K^*| = 2^{256} - 1$ berechnen und damit die folgende Aufgabe angehen.

Aufgabe 2

a) Man prüfe, ob das Element $X \in K^*$ die multiplikative Gruppe K^* erzeugt. (Dazu schaue man nach, ob für einen Primteiler $p / |K^*|$ schon gilt: $a^{\frac{|K^*|}{p}} = 1$)

b) In diesem Aufgabenteil soll das Diffie Hellman Protokoll in der von X erzeugten Untergruppe von K^* ablaufen. (Je nach Ergebnis von 2a könnte es sich bei dieser Untergruppe auch um ganz K^* handeln.)

A besitze denselben geheimen Schlüssel $a \in \mathbb{N}$ und B benutze dieselbe Zufallszahl $k \in \mathbb{N}$ wie in Aufg. 1.

Man berechne jetzt den geheimen Schlüssel von A, den Mailheader und den Kommunikationsschlüssel in K^* und überprüfe in K^* die Gleichung $\left(X^a\right)^k = \left(X^k\right)^a$ und versuche dabei, Pari so zu programmieren, daß die resultierenden Polynome aus $\mathbb{Z}_2[X]$ in natürlicher Weise als Bitstrings ihrer Koeffizienten dargestellt werden.

c)
Man finde ein Element der Ordnung 257 in K^*!
Anleitung: Es ist $257 \cdot q = 2^{256} - 1$. Man findet in der additiven Gruppe $\mathbb{Z}_{257} \times \mathbb{Z}_q$ leicht ein Element der Ordnung 257. Dieses läßt sich über den chinesischen Restesatz als Element von $\mathbb{Z}_{2^{256}-1}$ und über den Gruppenhomomorphismus $\mathbb{Z}_{2^{256}-1} \to K^*,\ k \to X^k \bmod f$ als Element von K^* wiederfinden.

Aufgabe 3 (freiwillig, ggf. Vortrag im Projektplenum)
Man generiere einen PGP-Schlüssel, beschaffe sich die entsprechende Dokumentation und extrahiere die öffentlichen und privaten Diffie-Hellman Schlüssel. (Man muß eine leere Passphrase setzen, um an den privaten Schlüssel im Klartext heranzukommen.)