RUHR
UNIVERSITÄT
BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Alexander Meurer, Ilya Ozerov

Hausübungen zur Vorlesung

Kryptanalyse

WS 2011/2012

Blatt 5 / 16. November 2011 / Abgabe bis spätestens 23. November 2011, 10 Uhr in dem Kasten auf NA 02

AUFGABE 1 (5 Punkte)**:**
Zeigen Sie, dass Aufgabe 3 der 5. Präsenzübung auch ohne Kenntnis von c_5 lösbar ist.

AUFGABE 2 (5 Punkte)**:**
Sei N ein RSA-Modul und $e = 3$ der öffentliche Exponent. Seien $m_1, m_2 \in \mathbb{Z}_N$ mit $f(m_1) = m_2 \bmod N$ für eine affine Abbildung $f : \mathbb{Z}_N \to \mathbb{Z}_N$, d.h. $f(x) = a \cdot x + b \bmod N$ wobei wir $a \in \mathbb{Z}_N^*$ und $b \neq 0$ voraussetzen.
Zeigen Sie: Sind $c_1 = m_1^e \bmod N$ und $c_2 = m_2^e \bmod N$ sowie a, b (also f) bekannt, so können wir m_1 und somit auch $m_2 = f(m_1)$ effizient berechnen.

Hinweis: Definieren Sie sich geeignete Polynome g_1, g_2, die die einzige Nullstelle m_1 haben (mit Begründung!) und nutzen Sie aus, dass Sie $\mathrm{ggT}(g_1, g_2)$ effizient berechnen können.

AUFGABE 3 (5 Punkte)**:**
Sei $N = pq$ ein RSA-Modul und $b = a^2 \bmod N$. Konstruieren Sie einen Algorithmus, der bei Eingabe b, N in Zeit $\tilde{\mathcal{O}}(N^{\frac{1}{2}})$ und Platz $\tilde{\mathcal{O}}(1)$ eine Quadratwurzel von b berechnet. Verwenden Sie dazu den Satz von Coppersmith (Satz 60).

Hinweis: Es kann hilfreich sein, zunächst die Existenz einer Approximation A von a einer gewissen Güte N^δ anzunehmen. Die Approximationen kann man dann per Brute-Force durchgehen.

AUFGABE 4 (5 Punkte)**:**
Wir erinnern uns an Aufgabe 3 aus der ersten Hausübung. Mittlerweile hat Alice ihren Fehler eingesehen und verschickt nicht mehr identische Nachrichten an 17 verschiedene Adressaten. Sie möchte stattdessen nur Bob eine persönliche Nachricht schicken, welche sie erneut symmetrisch verschlüsselt. Den zugehörigen 80 Bit Schlüssel k verschlüsselt Alice mit Bobs öffentlichem Schlüssel N und e = 17 mit RSA. Sie paddet den Schlüssel nach dem alten Schema, d.h. wir haben die Binärdarstellung

`m=10.....0[k_79..k_0]`

wobei die führende 1 von 0en in Position 1999 bis 80 gefolgt wird. Der Schlüssel ist dann in den letzten 80 Bit der Nachricht enthalten, d.h. $c = (2^{2000} + k)^e \bmod N$.

(a) Eve fängt erneut das Chiffrat c ab. Zeigen Sie mit Hilfe von Satz 59 aus der Vorlesung, dass Eve unter Ausnutzung der Paddingstruktur aus dieser einzigen Nachricht den Schlüssel k extrahieren kann.

(b) Implementieren Sie den Angriff in sage. Was ist die minimale Wahl für m? Wie ist dann die Dimension des Gitters? Wie lautet der gesuchte Schlüssel k zur Eingabe

```
N=176011665164614367747018792045186455424932971112472869172229316930
08234041384417178059445003224580161890156906120342437674460673498731
69809588156916493915892440155764374731001651211889221010648358430845
28413300665877255048566896792792055608883850068468596099709510668276
30642361383000385698754714735587108480550378279238636750051100432886
72310189994440609062621084729582503794046821590432154358137378200657
82194737478469311244023409343479184113014878141959318356288136198673
36680993414302937944885396736882204545042678127517460457587321837802
20386800597287070495915520710202294761210532451798783643762414776242
58337453

c=172902639785848924058640506651789807482753743644835437388020679696
76340588249338111515889012976678487829734088145525523061733357502362
57145662935537378928946981670214501650078106901242593510838130520912
51150227997438560627541851171415683552188989270697791942146151816499
25958321099567494637914953501750777665221209479693794340263041730469
57246466788027121544736544846368966286490229227633292512761560674365
88361962290642716448722144622918263987529666119630603869953615341855
11725314450678368692694922990056048766750620504131090097308915256698
78021683883845173195212827003579578343212985148857762223023301457034
2030648
```

und öffentlichem Exponenten `e=17`? Geben Sie den Quelltext Ihres Programms mit ab. Sie finden die Eingabeinstanz wie gewohnt auf der Webseite in den Dateien `H5N.sobj`, `H5e.sobj` und `H5c.sobj` oder `padding.txt`.