Übungen zur Vorlesung Kryptologie
Prof. Dr. Klaus Reinhardt / Dr. Bernd Borchert

WS 2013/14
Universität Tübingen
20.12.2010

8. Übungsblatt

Aufgabe 1.
Wie lautet der Pseudocode eines Algorithmus zur Zerlegung von n in Primfaktoren unter Verwendung eines Primzahltests ISPRIM(n) und eines Algorithmus SPLIT(n), der, falls möglich, zwei nichttriviale Faktoren von n liefert.

Aufgabe 2
Es sei bekannt, daß der Angreifer auf den RSA-Schlüssel Pollard's (p-1)-Faktorisierung bis $B = 1000000$ versucht. Welche Sicherheitsmaßnahme sollte man bei der Schlsselerzeugung mindestens ergreifen?

Aufgabe 3.
Ein naiver RSA-Anwender mache den Fehler p und q nur in einem Abstand von 1000000 zu suchen. Wie kann dies ein Angreifer ausnutzen? (Algorithmus unter Verwendung der quadratischen Faktorisierung als Pseudocode).

Aufgabe 4.
Faktorisiere 73543 mit der quadratischen Siebfaktorisierung.

Aufgabe 5.
In der Praxis wird bei der quadratischen Siebfaktorisierung ein mit x indiziertes Array verwendet, in dem durch logarithmische Gewichtung für jedes p der Faktorbasis für jedes x die Wahrscheinlichkeit dafür daß $q(x)$ glatt ist, vorab geschätzt wird. Wie kann dieser Siebvorgang als Pseudocode beschrieben werden?

Aufgabe 6
Faktorisiere 401963 mit dem Wissen, dass $\phi(401963) = 400680$.

Aufgabe 7
Faktorisiere 11413 unter Kenntnis des RSA-Schlüsselpaares $(3533, 11413), (6597, 11413)$.

Aufgabe 8.
Welche Wurzeln hat 1 modulo $31 \cdot 17$?

Aufgabe 9.
Seien ω_1 und ω_2 die nichttrivialen Wurzeln von 1 für das n aus dem Rabin-Schlüssel $K = (n, p, q, B)$ und x die Nachricht. Was sind die 3 anderen Werte, die die Entschlüsselung von $e_K(x)$ liefert?

Aufgabe 10.
Berechne den diskreten Logarithmus von 24 zur Basis 2 für den Modulus 97 mit Shank's Algorithmus.