

## 2. Übungsblatt

### Aufgabe 19.

Faktorisiere 1751 mit der Rho-Faktorisierung

### Aufgabe 20.

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 21

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 Schlüsselerzeugung mindestens ergreifen?

### Aufgabe 22.

Ändere den Algorithmus von Aufgabe 8 so ab, daß Primzahlen  $p$  mit  $(p-1)/2$  prim gefunden werden.

### Aufgabe 23.

Ein naiver RSA-Anwender mache den Fehler  $p$  und  $q$  sehr nahe beieinander zu verwenden. Wie kann dies ein Angreifer ausnutzen? (Algorithmus unter Verwendung der quadratischen Faktorisierung als Pseudocode).

### Aufgabe 24.

Faktorisiere 73543 mit der quadratischen Siebfaktorisierung.

### Aufgabe 25.

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 26

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

### Aufgabe 27

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

### Aufgabe 28.

Welche Wurzeln hat 1 modulo  $31 \cdot 17$  ?

### Aufgabe 29.

Seien  $\omega_1$  und  $\omega_2$  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 30.

Ein Las Vegas Algorithmus habe die Erfolgswahrscheinlichkeit  $\epsilon$ . Wie groß ist die Wahrscheinlichkeit, beim  $n$ -ten Versuch zum ersten mal Erfolg zu haben? Wie oft muß der Algorithmus wiederholt werden, damit die Erfolgswahrscheinlichkeit  $\delta$  wird? (Sei  $\delta > \epsilon$ .)

### Aufgabe 31.

Seien  $f$  und  $g$  injektive Einwegfunktionen. Ist dann auch  $h$  mit  $h(x) = f(g(x))$  Einwegfunktion?