Attacks against RSA signatures

Jean-Sébastien Coron

Université du Luxembourg

1 Fault attacks against RSA signatures

1. Implement the signature generation algorithm using the Chinese Remainder Theorem (CRT) using the Sage library. More precisely, to compute $s = m^d \bmod N$, compute

$$s_p = s \mod p = m^{d \bmod p-1} \mod p$$

   and

$$s_q = s \mod q = m^{d \bmod q-1} \mod q$$

   Recover $s \bmod N$ from s_p and s_q using the CRT.
2. Assume that an error occurs during the computation of s_p, that is, an incorrect value $s'_p \neq s_p$ is computed while s_q is correctly computed. Explain and implement how to recover the factorization of N from s, following the Bellcore attack [BDL97].
3. How could such error be detected ? Propose and implement a simple method to detect such error.

2 Optional: the Desmedt-Odlyzko attack

Implement the Desmedt-Odlyzko attack [DO85] described in the lecture, with the RSA signature scheme $\sigma = H(m)^d \mod N$. The attack computes a forged signature as a multiplicative combination of existing signatures.

For simplicity the hash function can be computed as follows:

```
import hashlib

def sha1(s,digestsize=50):
  m = hashlib.sha1()
  m.update(s)
  return Integer(m.hexdigest(),base=16) % 2^digestsize
```

To detect smooth numbers among $H(m_i)$, one can use the `factor()` function from Sage. Given a $(\ell+1) \times \ell$ matrix $\boldsymbol{M}$ of exponent vectors modulo e, one can obtain a vector from the kernel of M using:

```
v=Matrix(GF(3),M).left_kernel().matrix()[0]
```

assuming that we work with public exponent $e = 3$. Using such vector $\boldsymbol{v}$ one can then express one row of $\boldsymbol{M}$ as a linear combination of the others. This enables to express one $H(m_\tau)$ as a multiplicative combination of the others. Eventually, this enables to express one signature as a multiplicative combination of the others, hence a forgery.

To test the attack, one can use small parameters, for example `digestsize`=50, and a number of primes $\ell = 100$. It can be interesting to optimize the running time by varying ℓ for a fixed `digestsize`. Eventually, one can experiment the attack for increasing values of `digestsize`.

References

[BDL97] Dan Boneh, Richard A. DeMillo, and Richard J. Lipton. On the importance of checking cryptographic protocols for faults (extended abstract). In *Advances in Cryptology - EUROCRYPT '97, International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 11-15, 1997, Proceeding*, pages 37–51, 1997.

[DO85] Yvo Desmedt and Andrew M. Odlyzko. A chosen text attack on the RSA cryptosystem and some discrete logarithm schemes. In *Advances in Cryptology - CRYPTO '85, Santa Barbara, California, USA, August 18-22, 1985, Proceedings*, pages 516–522, 1985.