2.10 More Attacks

Finally we give a short overview over some other attacks on RSA. For a comprehensive treatment consult the paper by D. Boneh (see the introduction of this section):

1. **Small private exponent:** M. Wiener detected a way of efficiently computing the private key d from the public key (n, e) using continued fractions in the case $d < \frac{1}{3} \cdot \sqrt[4]{n}$.

2. **Related plaintexts** after Franklin/Reiter. Assume two different plaintexts a_1 and a_2 are related by an affine equation $a_2 = sa_1 + t$ with known coefficients s, $t \neq 0$. Then the corresponding plaintexts are efficiently computable from the public key (n, e), the coefficients s and t and the ciphertexts. Coppersmith found a situation that forces such an affine equation in the case where a_1 and a_2 originate from the same plaintext by "padding" differently.

3. **Partial leak** after Boneh/Durfee/Frankel/Coppersmith. If the last quarter of the bits of one of the integers d (the private exponent), p, or q (the prime factors of the module) are known, then n may be efficiently factorized.

4. **Timing and power attacks** after Kocher. The attacker observes the CPU during a decryption and measures the execution time or the power consumption. From this she gains informations about the bits of the private exponent. See the binary power algorithm, Section 1.2.

5. **Differential fault analysis** after Shamir et al. The attacker exposes the processor (for instance a smartcard) to environment conditions slightly outside the range where the specification guarantees a faultless operation, for instance by deforming, heating, radiation. Then the processor will produce single faulty bits that allow statistical inferences about the internal parameters.

Other attacks don't target the RSA algorithm itself but bugs in the implementation, faulty use in cryptographic protocols, flawed interaction with the system environment, and other mistakes.

In some situations using modules with more then two prime factors might even be advantageous, as the following paper suggests:

- M. Jason Hinek, Mo King Low, Edlyn Teske: On some attacks on multi-prime RSA. SAC 2002, 385–404.