2.9 The Signature Trap

The signature trap doesn't challenge the security of RSA itself, but the frame conditions of its use: Since reversing the order of encryption and decryption is the basic mechanism of digital signatures the user has to take care that he doesn't inadvertently decrypt a ciphertext in the erroneous belief that he digitally signs a document. Would the standard input to the signature algorithm be a normal plaintext, the user would realize this situation at once. However for (at least) three reasons the situation is different:

1. To get acceptable performance usually a digital signature is applied to a (cryptographic) hash value of a document. This cannot be distiguished from a random bitstring.

2. Strong authentication requires digitally signing a random bitstring instead of entering a password to prove the user's identity. Even if the result was a decrypted plaintext—the user wouldn't see it at all since it is immediately sent to the communication partner (that might be a server, or a "man in the middle").

3. Moreover the attacker could present an arbitrary text that is "camouflaged" by some kind of encryption, and require the user to "sign" (i. e. decrypt) it. Even a close inspection of the result would not detect the fraud—see below. This is a otherwise very useful property of RSA: It is the basis for blind signatures and hence the generation of digital pseudonyms and anonymous transactions.

By the way this an instance of an *attack with chosen ciphertext*. To escape this attack in practice each of the three (or four) functions

- encryption,
- digital signature,
- strong authentication,
- (optionally) blind signature,

should use a different key pair.

Now for the "camouflage" that disguises the chosen ciphertext attack. Here is the procedure:

1. The attacker M ("Mallory") has an intercepted ciphertext $x = E_{\mathrm{A}}(a)$ and would like to read it. He encrypts it as $y = C(x)$ using a function C known only to him.

2. He presents y to his victim A ("Alice") and requires a digital signature. A generates $z = D_{\mathrm{A}}(y)$.

3. M removes the "camouflage" by a suitable inverse transformation C'. For this he needs a pair (C, C') of transformations such that

$$C' \circ D_{\mathrm{A}} \circ C = D_{\mathrm{A}}.$$

   Then $a = D_{\mathrm{A}}(x) = C'(z)$.

As a peculiarity of RSA such pairs (C, C') of transformations exist: Let $E_{\mathrm{A}}(a) = a^e \bmod n$, and take C as the shift by u^e on $\mathbb{M}_n = (\mathbb{Z}/n\mathbb{Z})^\times$, and C' as the multiplication by $u^{-1} \bmod n$ where $u \in \mathbb{M}_n$ is randomly chosen. Thus the attack runs through the steps:

1. M chooses u und computes $y = C(x) = u^e x \bmod n$.
2. A generates $z = y^d \bmod n$.
3. M computes

$$C'(z) = zu^{-1} = y^d u^{-1} = u^{ed} x^d u^{-1} = x^d = a$$

   in $\mathbb{Z}/n\mathbb{Z}$.