Chapter 13
Certified Signatures

Here we learn how certified signatures can be attached to secret messages in the context of public-key encryption. The degree of certitude (in the sense of avoiding random confusions) achievable by this method, which is based on modular arithmetic, appears to exceed by far that of notarized signatures, fingerprinting or, conceivably, even genetic analysis.

Certified signatures are also important in protecting computer systems against illicit entry and manipulation, and safeguarding data files from unauthorized "readers", falsification or destruction.

13.1 A Story of Creative Financing

Baron von Münchhausen, a close relative of the fabulous liar of the same name, and founder of the Georg-August University at Göttingen under the auspices of his King in Hanover, Georg August[1], received a secret message in (say) 1743 saying (in part):

"SPEND ALL EXCESS FUNDS OF KINGDOM ON NEW UNIVERSITY IN GOTTINGEN." signed "GEORGE".

How does von Münchhausen know that it was really King George who sent that generous but unlikely message? George is about to establish two more institutions of higher learning in his American colonies: King's College on an island called Manhattan (later to be known as Columbia University) and the College of New Jersey (now Princeton University) and the royal treasure has few, if any, "excess funds" to throw in the direction of Göttingen. The signature looks fine, but it could have been faked.

13.2 Certified Signature for Public-Key Encryption

In one of the great advances of modern secure and reliable communication (apart from public-key encryption itself), *certified signatures* can now be attached to public-key encryption messages in such a manner as to remove any doubt about

[1] Also known in London as George II, King of England, etc., etc.

M. Schroeder, *Number Theory in Science and Communication*, 5th ed.,
DOI 10.1007/978-3-540-85298-8_13,

the sender [13.1]. This works as follows: The sender, call him N, encrypts his name, address, etc., by his *de*crypting key t_0 (which only he knows!). Thus, he forms

$$S \equiv N^{t_0} \pmod{r_0}, \tag{13.1}$$

which he appends to his message M (which includes his name) and encrypts both M and S by the (public!) encrypting key of the receiver s_1, r_1.

The receiver decrypts using his secret key t_1, and reads the message M followed by a string of "garbled" symbols S, which must be the certified signature, because the message was identified as carrying such a signature. The message also purports to have been sent by N. Thus, knowing the protocol, the receiver applies the publicly known encrypting parameters of N, namely s_0 and r_0, to S and obtains

$$S^{s_0} \equiv N^{t_0 s_0} \equiv N \pmod{r_0}, \tag{13.2}$$

i. e., the name and address, etc., of the sender. And no one, but no one, who did not know t_0, could have constructed S so that with the above operation it would yield N. A certified signature to put all other "certified" signatures – including fingerprinting and (present-day) genetic analysis – to shame!

The reader can find further information on digital signatures and authentications to counteract potential threats[2] in financial, diplomatic and military "transactions" in [13.2–4].

With the spread of the Internet and electronic banking, data security and guaranteed signatures have taken on a wholly new dimension, see [13.5]. Proof of purchase and the important concept of "oblivious transfer" on the Internet are discussed in [13.6]. See also [13.7].

[2]

reneging	the *originator* subsequently disowns a transaction
forgery	the *recipient* fabricates a transaction
alteration	the *recipient* alters a previous valid transaction
masquerading	an *originator* attempts to masquerade as another