Here we describe a public-key digital encryption scheme that does not require secret-key distribution - one of the Achilles' heels of secret-key cryptographic systems because once the secret encrypting key becomes known, transmissions are no longer secret. Figure 9.1 illustrates the situation for a generic encryption/decryption system. Both transmitter and receiver need to be in possession of the same key, a long string of “random” binary digits. At the transmitter, on the left, these bits (0 or 1) are added modulo 2 to the message bits to form the encrypted message. A “bad guy” tapping into the output cannot decrypt the transmitted cryptogram unless the knows the key. In fact, he does not even know whether there is traffic on the tapped line: even if there is no traffic (a “message” consisting only of 0’s) the line still carries random 0’s and 1’s. (This disguise of traffic volume is itself an important asset of the illustrated encryption method – many impending enemy actions have been betrayed simply by a rise in traffic.)

The problem implicit in the illustrated method is of course the secure transportation or transmission of the key between sender and receiver. Many ingenious schemes have been invented to solve the key problem. In addition the keys have to be protected from enemy ogling. To forestall illicit snooping, the navies of the world print sensitive keys on water-soluble paper. In other words, the key will dissolve into thin water when the ship sinks. A great idea – but not all vessels will sink when attacked by the enemy. Figure 9.2 shows a case in point: His Majesty’s Ship, the German light cruiser *Magdeburg*, run
aground off the Baltic Coast in August 1914 while trying to outmaneuver a Russian man-of-war. The poor *Magdeburg* refused to sink and the Russians got hold of the undissolved key book of the imperial German Navy (see Fig. 9.3). After examining it for several weeks, they shipped it to the British Admiralty (First Lord none other than Winston Churchill) who could make excellent use of it.

This kind of mishap is completely avoided if there is no secret key to be kept secret. In fact, in public-key encryption, every potential recipient of secret messages *publishes* his encrypting key (hence the name *public* key). But knowledge of the encrypting key is of no practical help in decryption. The public-key is the key to a “trap door” through which messages can vanish, not to be recovered – except through a different route to which only the legitimate receiver holds the required key, the decrypting key. (Trap door means easily in, but out only with the proper tools.) It is as if everyone had a (chained!) box in front of his house into which secret messages could be stuffed and to which only the owner had the proper opening key.

The required trap-door behaviour is realized for digital messages (represented by long strings of digits) by the fact that it is easy to multiply two large numbers, but impossible to factor sufficiently large numbers in a reasonable amount of time.

The public-key cryptographic systems described here are based on modular arithmetic, requiring knowledge of the Euler $\phi$ function of the modulus