Chapter 28
Fermat’s Little Theorem

We begin this chapter with a fundamental result of number theory, discovered by Pierre de Fermat. Fermat lived from 1601 to 1665. Many of his contemporaries were “number-lovers” rather than number theorists, [108, p. 51], and one thing that interested them was perfect numbers (a number is perfect if it is the sum of all its proper divisors). Bernard Frénicle de Bessy, who was also a mathematician and physicist, first raised the question of whether there was a perfect number of 20 digits and, if not, what the next largest perfect number was. (See [29] and [30].) The answer to the question required determining whether certain large numbers were prime. As a consequence, the men began corresponding. In a letter to Frénicle, dated October 18, 1640, Fermat stated what is now known as Fermat’s theorem or Fermat’s little theorem (to distinguish it from Fermat’s last theorem), but he did not include a proof. In 1736, almost a century later, Leonhard Euler gave the first rigorous proof of the little theorem. Though this theorem is clearly theoretical in nature, it plays an important role in primality testing; that is, in deciding whether or not a certain number is prime. Fermat’s little theorem (in the form due to Euler) is also the mathematical heart of the widely used RSA code that we will describe later in this chapter. In fact, Fermat’s little theorem is not little at all.

Theorem 28.1 (Fermat’s Little Theorem). *Let p be a prime and let a be an integer satisfying* $\gcd(a,p)=1$. *Then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Exercise 28.2. Verify Theorem 28.1 for a few values of p and a. ○

We will state and prove Euler’s generalization of this theorem below. Fermat’s little theorem will then follow as a special case.

In order to state the form of the theorem that we will prove, we will introduce a new function: **Euler’s ϕ-function** is the function $\phi : \mathbb{Z}^+ \to \mathbb{Z}^+$ where $\phi(n)$ denotes the number of integers k, with $0 \le k < n$, that are relatively prime to n.

U. Daepp and P. Gorkin, *Reading, Writing, and Proving: A Closer Look at Mathematics*, Undergraduate Texts in Mathematics, DOI 10.1007/978-1-4419-9479-0_28,

Exercise 28.3. Calculate $\phi(1), \phi(12), \phi(7), \phi(13)$, and $\phi(7 \cdot 13)$. ○

Exercise 28.4. Show that if p is prime, then $\phi(p) = p - 1$. ○

The following lemmas will assist us in our proof of Theorem 28.7 below. The first lemma requires the multiplication in $\mathbb{Z}_n$ that we defined in Chapter 27.

Lemma 28.5. *Let n and a be integers satisfying $n > 1$ and $\gcd(a,n) = 1$. If r and s are integers satisfying $ar \equiv as \pmod{n}$, then $r \equiv s \pmod{n}$.*

Proof. Since $\gcd(a,n) = 1$, we may apply Corollary 27.11 to obtain an integer b such that $ab \equiv 1 \pmod{n}$. We now multiply the equivalence $ar \equiv as \pmod{n}$ by b to get $arb \equiv asb \pmod{n}$. Using commutativity of the multiplication (see Problem 27.14) and simplifying, we obtain $r \equiv s \pmod{n}$, as desired. □

We summarize much of what we have learned below.

Lemma 28.6. *Let a and n be integers with $n > 1$ and $\gcd(a,n) = 1$. Then there exist exactly $\phi(n)$ distinct integers, $m_1, m_2, \ldots, m_{\phi(n)}$ such that*

(i) $0 \le m_i < n$ *and* $\gcd(m_i, n) = 1$ *for* $i = 1, \ldots, \phi(n)$,

(ii) there exists $c \in \mathbb{Z}$ such that

$$\left(\prod_{i=1}^{\phi(n)} m_i\right) c \equiv 1 \pmod{n}, \text{ and}$$

(iii) $am_i \not\equiv am_j \pmod{n}$ *for* $i \ne j$.

Proof. By the definition of Euler's ϕ-function, there exist exactly $\phi(n)$ distinct integers satisfying (i).

Using Problem 28.1, it follows from property (i) that $\gcd(\prod_{i=1}^{\phi(n)} m_i, n) = 1$. Thus we may apply Corollary 27.11 to obtain an integer c such that

$$\left(\prod_{i=1}^{\phi(n)} m_i\right) c \equiv 1 \pmod{n},$$

completing the proof of (ii).

For part (iii) recall that $\gcd(a,n) = 1$. Now $m_1, \ldots, m_{\phi(n)}$ are distinct integers with $0 \le m_k < n$ for each k. So, if $i \ne j$, then $m_i \not\equiv m_j \pmod{n}$. Thus (the contrapositive of) Lemma 28.5 implies that $am_i \not\equiv am_j \pmod{n}$ for $i \ne j$. □

Now we are ready for Euler's generalization of Fermat's little theorem.

Theorem 28.7 (Euler's Theorem). *Let $a, n \in \mathbb{Z}$ with $n > 1$. If $\gcd(a,n) = 1$, then*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Proof. Let $m_1, m_2, \ldots, m_{\phi(n)}$ be as in Lemma 28.6. Then $am_1, am_2, \ldots, am_{\phi(n)}$ are distinct integers $\pmod{n}$, and $\gcd(m_i, n) = 1$. Note that since there are $\phi(n)$ integers, we have

$$a^{\phi(n)} \prod_{i=1}^{\phi(n)} m_i = \prod_{i=1}^{\phi(n)} (am_i). \tag{28.1}$$

Thus, if we can find $\prod_{i=1}^{\phi(n)} (am_i)$ as well as the reciprocal of $\prod_{i=1}^{\phi(n)} m_i \pmod{n}$, we can also compute $a^{\phi(n)} \pmod{n}$.

To compute the product in equation (28.1), use Exercise 27.7 to obtain $\phi(n)$ integers, $s_1, s_2, \ldots, s_{\phi(n)}$ such that $s_i \equiv am_i \pmod{n}$ and $0 \le s_i < n$. Now, $\gcd(a, n) = 1$ and $\gcd(m_i, n) = 1$, so by Problem 28.1, $\gcd(am_i, n) = 1$. Thus, Lemma 27.12 implies that $\gcd(s_i, n) = 1$. We have found $\phi(n)$ different integers, $s_1, s_2, \ldots, s_{\phi(n)}$, all relatively prime to n. So $s_1, s_2, \ldots, s_{\phi(n)}$ is simply a (possible) reordering of $m_1, m_2, \ldots, m_{\phi(n)}$. Consequently

$$\prod_{i=1}^{\phi(n)} (am_i) \equiv \prod_{i=1}^{\phi(n)} s_i \equiv \prod_{i=1}^{\phi(n)} m_i \pmod{n}. \tag{28.2}$$

Combining (28.1) and (28.2) we get

$$a^{\phi(n)} \prod_{i=1}^{\phi(n)} m_i \equiv \prod_{i=1}^{\phi(n)} m_i \pmod{n}. \tag{28.3}$$

By Lemma 28.6, there is an integer c such that $(\prod_{i=1}^{\phi(n)} m_i)c \equiv 1 \pmod{n}$. So, multiplying both sides of (28.3) by c, we obtain

$$\left(a^{\phi(n)} \prod_{i=1}^{\phi(n)} m_i\right) c \equiv \left(\prod_{i=1}^{\phi(n)} m_i\right) c \pmod{n}.$$

Using associativity and simplifying, we obtain $a^{\phi(n)} \equiv 1 \pmod{n}$, as desired. □

Since Fermat's little theorem is a special case of Euler's theorem, with $n = p$ for a prime p and $\phi(p) = p - 1$, we now have a proof of Theorem 28.1 as well.

One interesting application of Euler's theorem is in an area of mathematics known as coding theory. Here's the idea: Suppose you want to transmit a message to a receiver, whom we shall refer to as Henry, in such a way that no one else can read it. This is done all the time. (Just think how often you have sent your credit card number over the Internet!) The idea is to use a code that is difficult to decode. But of course, if it's too difficult, Henry won't be able to decode it either. Applying the code to our secret message is like applying a function. Henry needs to undo the code, or mathematically speaking, apply the inverse function. So we need something like a function that has an inverse, but whose inverse is very difficult to find. Such functions are called trapdoor functions. (Anyone can get in, but only Henry can get out.) Since it is virtually impossible to find the inverse function, the original function used to hide the message can be made public. This is achieved using a method called a public key encryption, which includes a public key and a private key.

One particular trapdoor function leads to the following method. Henry, the receiver of the messages, decides on a function that is determined by the two integers, n and e, called the key of the code. Anybody who is interested can learn about these two numbers (this is why it is a *public key encryption*). If you want to send a message to Henry, then you first turn the English text into a positive integer m, called the plaintext. There are standard ways to do this, but the number produced does not yet hide the message. (If the translation leads to a number m that is greater than n, the message must be divided into several smaller messages.) The plaintext, m, must now be scrambled so that its meaning cannot be deciphered by anyone except Henry. Or, mathematically speaking, we have to apply the trapdoor function to it. A simple but very safe way to do this, is to change m to $m^e \pmod{n}$. It's interesting to note that though it appears that everyone has all the information Henry has, it turns out that Henry knows something no one else knows. We'll explain this once we tell you how Henry will unscramble the message. So the question is: How can Henry recover m from $m^e \pmod{n}$? It turns out that he will use Euler's theorem. Here's how:

Example 28.8. Let m, n, and e be positive integers satisfying $n > 1$, $\gcd(m,n) = 1$, and $\gcd(e, \phi(n)) = 1$. Find a positive integer d such that $(m^e)^d \equiv m \pmod{n}$.

Why is this example relevant? Well, once you have d, you have m^e, n, e, and d. You can then calculate $(m^e)^d$, which (as we learned in this example) is equivalent to m modulo n.

In order for the solution to this problem to be useful, we need a constructive way to find d. We claim that (i) we can find an integer d such that $e \cdot d \equiv 1 \pmod{\phi(n)}$ and that (ii) any such integer will fulfill the requirement $(m^e)^d \equiv m \pmod{n}$.

Now since e is a positive integer relatively prime to $\phi(n)$, Theorem 27.6 guarantees the existence of integers k and l such that $1 = ke + l\phi(n)$. Let d be the smallest positive integer such that $d \equiv k \pmod{\phi(n)}$. Then $1 \equiv de \pmod{\phi(n)}$, which is what we needed to show.

For part (ii), calculate $(m^e)^d = m^{ed}$, and recall that $m^{\phi(n)} \equiv 1 \pmod{n}$, by Euler's theorem. We just showed that $1 = ed + j\phi(n)$ for some $j \in \mathbb{Z}$, so

$$m^{ed} = m^{1-j\phi(n)} = m \cdot (m^{\phi(n)})^{-j} \equiv m \cdot 1 \equiv m \pmod{n}.$$

Note that in Problem 27.20 we gave a constructive method to find the integers k and l used above, and in Exercise 27.7, you showed how to get the integer d from k. ○

Now back to Henry. Remember that he has determined, rather carefully, his n and e and has given out these two integers. He also calculated the very important integer d from Example 28.8, but kept it a secret. Now you may well be asking the question, "Why can't everyone with access to n and e calculate d themselves, and then read the messages meant for Henry?" The reason is that in order to find d, a person needs to know the modulus that determines d, namely, $\phi(n)$. Henry knows (as you will once you work Problem 28.12) that if he chooses n such that it is the product of two primes p_1 and p_2, then $\phi(n) = (p_1 - 1)(p_2 - 1)$. So he lets p_1 and p_2 be two primes, each about 300 digits long, following current recommendations. (He must be a little careful choosing p_1 and p_2, but we will not go into that here.) Now he and everyone else knows the product n, but not p_1 and p_2. This is the trapdoor. Henry knows n, p_1, and p_2. So he can find $\phi(n)$. But everyone else only knows n, so they would have to find p_1 and p_2. It takes no time at all to multiply two 300-digit numbers, but you cannot factor the product in a million years, not even with supercomputers! There is a second reason that Henry had to know $\phi(n)$: he needed e to be relatively prime to $\phi(n)$.

There is one more thing that we should mention. In Example 28.8 we have the additional condition $\gcd(m,n) = 1$ (see also Problem 28.19). Thus, it appears from our solution above that we also need $\gcd(m,n) = 1$. Fortunately our decoding method still works if we have $n = p_1 p_2$ for two different primes p_1 and p_2 and $\gcd(m,n) = p_1$. If you work Project 29.13, you will prove this in Lemma 29.16.

Henry's method to get secure messages is called the RSA public key encryption, and Example 28.8 is the mathematical content of it. To learn more about this ingenious and widely used method, work Project 29.13 on the RSA Code.

Definition

Definition 28.1. Euler's ϕ-function is the function $\phi : \mathbb{Z}^+ \to \mathbb{Z}^+$ where $\phi(n)$ denotes the number of integers k, with $0 \le k < n$, that are relatively prime to n.

Solutions to Exercises

Solution (28.2). We calculate two examples.

1. Let $p = 5$ and $a = 7$. Then $7^4 = 2401 \equiv 1 \pmod{5}$.
2. Let $p = 13$ and $a = 8$. Then $8^{12} = 68719476736$. Now $8^{12} - 1 = 68719476735$ $= 13 \cdot 5286113595$. Hence $8^{12} \equiv 1 \pmod{13}$.

Solution (28.3). $\phi(1) = 1$.

The nonnegative integers smaller than 12 are all listed. We cross out the ones that are not relatively prime to 12: $\cancel{0}, 1, \cancel{2}, \cancel{3}, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11$. Hence $\phi(12) = 4$.

Similarly, $\phi(7) = 6, \phi(13) = 12$, and $\phi(7 \cdot 13) = \phi(91) = 72$.

Notice that, in these examples, for p and q different primes $\phi(p) = p - 1$ and $\phi(p \cdot q) = \phi(p) \cdot \phi(q)$. Are these coincidences?

Solution (28.4). Note that for p prime and a an integer with $0 \le a < p$, we have $\gcd(a, p) = 1$ if and only if $a \ne 0$. Thus $\phi(p) = p - 1$ for every prime p.

Spotlight: Public and Secret Research

Research in mathematics today is often done by professors who work at universities or colleges. People frequently work collaboratively, though they also sometimes work alone. They might communicate via e-mail, get together when they can, work together at institutes, or they may never even meet each other. Once their work is done, they write it up and send it to a journal. The editor of the journal sends it to carefully selected referees who read the paper. The author is responsible for the correctness of the mathematics in the paper, but the referee (whose identity is generally hidden from the author) determines the value of the work, the appropriateness of its placement in the journal, the originality of the mathematics, and often the correctness of the results. Once the paper appears, everyone has access to the results and proofs in the paper.

There are also other places where mathematical research is done. In the United States, the *National Security Agency* (NSA) refers to itself as the "leading employer" of nonacademic mathematicians. In Great Britain, there is the *Government Communications Headquarters* (GCHQ), the successor to the famous Bletchley Park where British code breakers were so successful in intercepting and reading Nazi attack plans. The mathematics done in a place like this might become the government's secret, and therefore may never be published. Public key encryption is an example of how such secrecy may hamper mathematical progress.

In 1976, Whitfield Diffie, Martin Hellman, and Ralph Merkle developed the idea of the public key. In 1977, Ronald Rivest, Adi Shamir, and Leonard Adleman gave us the RSA code. A couple of decades later, it became known that British mathematicians at GCHQ had worked out the encryption idea a few years earlier. James Ellis, Clifford Cocks, and Malcolm Williamson, all employed at GCHQ, had discovered public key encryption, but neither they nor their supervisors realized the power and widespread applicability of the method. Their results were considered top secret and were only circulated within the agency. A few years later, the world admired the "new" cryptosystem and celebrated the "originators" in the United States, [99, Chapter 6].

Some private companies also restrict their employees' publications. There are instances of researchers circumventing this restriction by publishing under a penname. In 1908, William S. Gosset, who worked for the Guiness Brewing Company in Dublin, published a paper under the name "Student" to avoid repercussions. The distribution Gosset introduced is now known as *Student's t-distribution* (or the Student t-distribution) and it has had a profound impact on statistical theory and practice.

To learn more about the interesting history of public key encryption we recommend [99, Chapter 6] or [61].

An in-depth treatment of Fermat's little theorem, Euler's theorem, and Euler's ϕ-function, as well as historical notes can be found in the text [15, pp. 91–96 and 123–150]. In [57, pp. 418–420 and 556–558] Fermat's theorem and Euler's theorem are put in context. For short biographies of Pierre de Fermat and Leonhard Euler, see the Web at [79]. For a biographical sketch of Euler and a delightful description of Euler's mathematics in the various fields, see [22]. A good source to learn more about Fermat's life and his mathematics is [66].

Problems

Problem# 28.1. (a) Let $a,b,s \in \mathbb{Z}$ such that $\gcd(a,s)=1$ and $\gcd(b,s)=1$. Show that $\gcd(ab,s)=1$.

(b) Let $n \in \mathbb{Z}^+$ and $a_1,\dots,a_n$, and s be integers such that $\gcd(a_k,s)=1$ for all integers k with $1 \le k \le n$. Show that $\gcd(\prod_{k=1}^n a_k, s)=1$.

Problem 28.2. Show that the conclusion of Fermat's little theorem (Theorem 28.1) may not hold if p is not prime.

Problem 28.3. Use Fermat's little theorem to show that for p a prime, every integer a with $a \not\equiv 0 \pmod{p}$ has a reciprocal modulo p.

Problem 28.4. In Problem 28.3 above you proved that if p is a prime, then every integer that is not equivalent to zero modulo p has a reciprocal modulo p.

(a) Find the reciprocals of $1,2,\dots,6$ modulo 7.
(b) Given a prime p, find all integers x with $1 \le x < p$ that are the reciprocals of themselves.
(c) Prove the following theorem:

Theorem 28.9 (Wilson's theorem). *If p is a prime, then* $(p-1)! \equiv -1 \pmod{p}$.

Problem 28.5. Prove the converse of Wilson's theorem, namely: For an integer $n > 1$, if $(n-1)! \equiv -1 \pmod{n}$, then n is prime. (Hint: The case $n = 2^2$ needs to be considered separately.)

Problem 28.6. (a) Let p and q be primes with $p \neq q$, and let a and b be two integers. Prove that if $a \equiv b \pmod{p}$ and $a \equiv b \pmod{q}$, then $a \equiv b \pmod{pq}$.

(b) Use part (a) to show that if p and q are prime numbers with $p \neq q$, and a is an integer satisfying $\gcd(a,pq)=1$, $a^p \equiv a \pmod{q}$, and $a^q \equiv a \pmod{p}$, then $a^{pq} \equiv a \pmod{pq}$.

Problem 28.7. In this problem, we show that the following converse of Fermat's little theorem is false: If a is a prime and $a^{m-1} \equiv 1 \pmod{m}$, then m is necessarily a prime.

Let $a=2, p=11$, $q=31$, and $m=pq$. Use Problem 28.6 part (b) to show that the statement above is false. (Note: You can verify this counterexample directly with a calculator or computer. If you use Problem 28.6 part (b) and do the modular exponentiation efficiently, the verification can be done easily by hand. The example is from [46].)

Problem 28.8. Let a and n be integers with $n > 1$ and $\gcd(a,n)=1$. Prove that there exists a smallest positive integer m such that $a^m \equiv 1 \pmod{n}$ and $m|\phi(n)$.

Problem 28.9. (a) Calculate $\phi(5^2), \phi(5^3)$, and $\phi(5^4)$.

(b) For p a prime and n a positive integer, show that $\phi(p^n) = p^n(1-1/p)$.

(c) Calculate $\phi(128)$.

Problem 28.10. Is Euler's ϕ-function additive; that is, for all $m,n \in \mathbb{Z}^+$ is it the case that $\phi(m+n) = \phi(m) + \phi(n)$? Prove it or give a counterexample.

Problem 28.11. This problem guides you through the proof of the fact that Euler's ϕ-function is in some sense multiplicative. More precisely, you will prove

Theorem 28.10. *Let m and n be integers such that* $m > 1$ *and* $n > 1$. *If* $\gcd(m,n) = 1$, *then* $\phi(mn) = \phi(m)\phi(n)$.

(a) Let k_1, k_2, l_1, and l_2 be integers satisfying $0 \le k_1, k_2 < n$ and $0 \le l_1, l_2 < m$. Show that if $k_1 m + l_1 n \equiv k_2 m + l_2 n \pmod{mn}$, then $k_1 = k_2$ and $l_1 = l_2$.

(b) Use the result of (a) to show that for each $a \in \mathbb{Z}$ there is exactly one element $(k,l) \in \mathbb{Z} \times \mathbb{Z}$ such that $0 \le k < n$, $0 \le l < m$, and $a \equiv km + ln \pmod{mn}$.

(c) For positive integers m and n, use (b) to conclude that

$$|\{(k,l) \in \mathbb{Z} \times \mathbb{Z} : 0 \le k < n, 0 \le l < m, \text{ and } \gcd(km+ln, mn) = 1\}| = \phi(mn).$$

(d) For $k,l \in \mathbb{Z}$ with $0 \le k < n$ and $0 \le l < m$, show that $\gcd(km+ln, mn) = 1$ if and only if $\gcd(k,n) = 1$ and $\gcd(l,m) = 1$.

(e) Use (c) and (d) to obtain the conclusion of Theorem 28.10.

Problem 28.12. Use the results of Problems 28.9 and 28.11 to answer the following.

(a) Let $m \in \mathbb{Z}$ and suppose $m = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$, where $p_1, p_2, \ldots, p_k$ are distinct primes and $a_1, a_2, \ldots, a_k$ are positive integers. Prove that

$$\phi(m) = m \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

(b) Calculate $\phi(5712200)$.

Problem 28.13. Prove that for $n \in \mathbb{Z}^+$, the Euler ϕ-function satisfies

$$\phi(2n) = \begin{cases} \phi(n) & \text{if } n \text{ is odd} \\ 2\phi(n) & \text{if } n \text{ is even} \end{cases}.$$

Problem 28.14. Use the formula from Problem 28.12 to show that for p prime and r a positive integer, $\sum_{d|p^r} \phi(d) = p^r$.

Problem 28.15. Let a, b, and c be integers such that $\gcd(a,b) = 1$ and $a|bc$. Prove that this implies that $a|c$.

Problem 28.16. Prove Theorem 28.1 directly by adapting the proof of Theorem 28.7 to this simpler situation.

Problem 28.17. In each of the two cases below, use the method of Example 28.8 to find an integer m with $0 \leq m < 33$ satisfying

(a) $m^3 \equiv 8 \pmod{33}$ and $\gcd(m, 33) = 1$;
(b) $m^{77} \equiv 15 \pmod{143}$ and $\gcd(m, 143) = 1$.

Problem 28.18. Show that the conclusion of Euler's theorem may not hold if $\gcd(a, n) > 1$.

Problem 28.19. Show that if x and y are integers and p is a prime, then

$$(x+y)^p \equiv x^p + y^p \pmod{p}.$$

(You may find the binomial theorem useful here. If so, you may use, without proof, the fact that the binomial coefficient $\binom{n}{k}$ is an integer for $k, n \in \mathbb{N}$ with $k \leq n$.)

Problem 28.20. The RSA code relies on being able to calculate $m^e \pmod{n}$ quickly. Fortunately, this is possible with an intelligent plan and with the help of a computer.

(a) Devise a plan to calculate m^{100} with the smallest number of multiplications by multiplying two (and only two) integers at a time. How many multiplications and divisions did you need? (You don't need to prove that the number of multiplications you require is the smallest.)
(b) To multiply or divide two integers of n digits each we need to do roughly n^2 operations. If m and n have 600 digits, how many operations are needed to calculate $m^{100} \pmod{n}$?
(c) Your computer is, most likely, capable of performing $2 \cdot 10^{10}$ operations per second. How long will it take to calculate your $m^{100} \pmod{n}$?

Problem 28.21. The RSA code can also be used as a signature. In doing so, the sender sends out n and d and keeps e for himself. You receive two messages, one is a plain message and the other is an encrypted message. You can check whether the two messages are the same, because you have n and d. So, if the encrypted message unscrambles to the plain one, then it must come from the sender—the only person who knows e.

In this problem, we'll look at a specific example: The public signature key is $n = 77$ and $d = 13$. The message you get is 8 with the encrypted form 50. Decide whether the message came from the sender. If it didn't, calculate the true pair of messages.

Of course the numbers here are much too small, and you would be able to calculate e easily. If n were a 600-digit number, then you would no longer be able to do so, but you could still decode the encrypted message with the given information in a reasonable amount of time. In fact, you can decode the message very quickly if you have a computer—basically instantaneously, if your computer is programmed to do so. Sending the plain text can usually be omitted, because the probability that a randomly generated text makes sense is zero. Thus, if the decoded text makes sense, the signature is (for all practical purposes) correct.