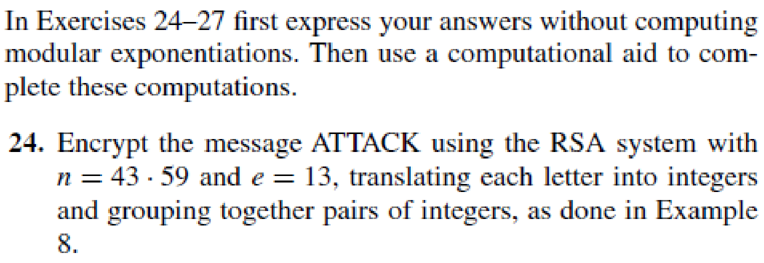
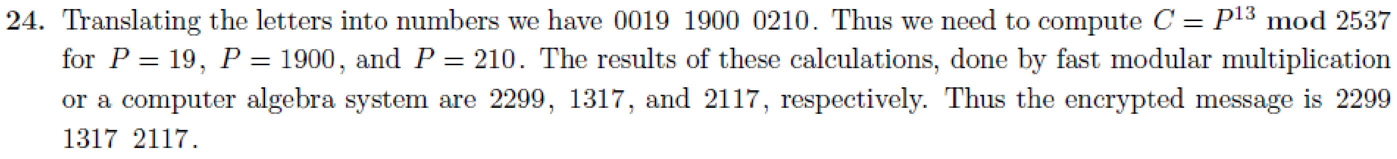
4.6 RSA

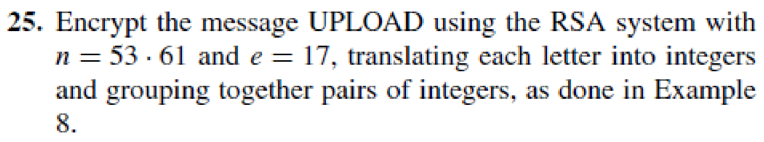


In Exercises 24–27 first express your answers without computing modular exponentiations. Then use a computational aid to complete these computations.

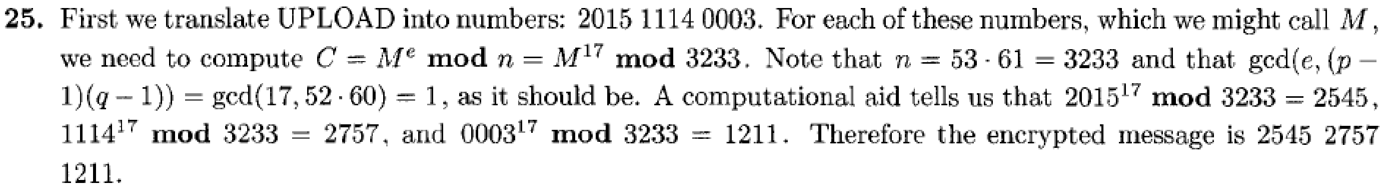
24. Encrypt the message ATTACK using the RSA system with $n = 43 \cdot 59$ and $e = 13$, translating each letter into integers and grouping together pairs of integers, as done in Example 8.



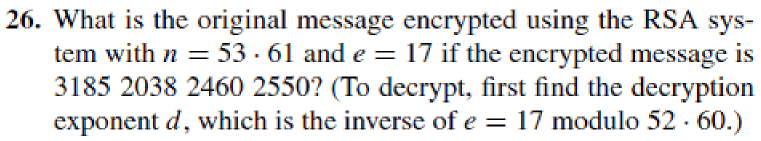
24. Translating the letters into numbers we have 0019 1900 0210. Thus we need to compute $C = P^{13}$ **mod** 2537 for $P = 19$, $P = 1900$, and $P = 210$. The results of these calculations, done by fast modular multiplication or a computer algebra system are 2299, 1317, and 2117, respectively. Thus the encrypted message is 2299 1317 2117.



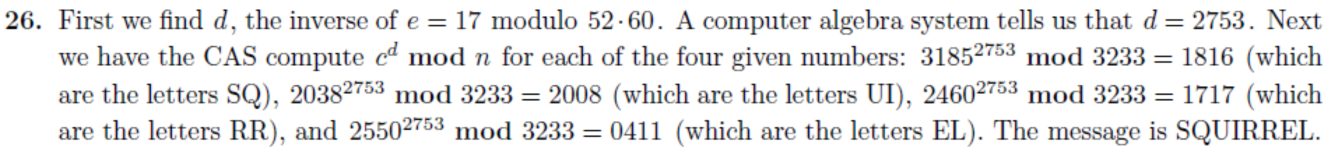
25. Encrypt the message UPLOAD using the RSA system with $n = 53 \cdot 61$ and $e = 17$, translating each letter into integers and grouping together pairs of integers, as done in Example 8.



25. First we translate UPLOAD into numbers: 2015 1114 0003. For each of these numbers, which we might call M, we need to compute $C = M^e \mathbf{\ mod\ } n = M^{17} \mathbf{\ mod\ } 3233$. Note that $n = 53 \cdot 61 = 3233$ and that $\gcd(e, (p-1)(q-1)) = \gcd(17, 52 \cdot 60) = 1$, as it should be. A computational aid tells us that $2015^{17} \mathbf{\ mod\ } 3233 = 2545$, $1114^{17} \mathbf{\ mod\ } 3233 = 2757$, and $0003^{17} \mathbf{\ mod\ } 3233 = 1211$. Therefore the encrypted message is 2545 2757 1211.



26. What is the original message encrypted using the RSA system with $n = 53 \cdot 61$ and $e = 17$ if the encrypted message is 3185 2038 2460 2550? (To decrypt, first find the decryption exponent d, which is the inverse of $e = 17$ modulo $52 \cdot 60$.)



26. First we find d, the inverse of $e = 17$ modulo $52 \cdot 60$. A computer algebra system tells us that $d = 2753$. Next we have the CAS compute c^d **mod** n for each of the four given numbers: $3185^{2753} \mathbf{\ mod\ } 3233 = 1816$ (which are the letters SQ), $2038^{2753} \mathbf{\ mod\ } 3233 = 2008$ (which are the letters UI), $2460^{2753} \mathbf{\ mod\ } 3233 = 1717$ (which are the letters RR), and $2550^{2753} \mathbf{\ mod\ } 3233 = 0411$ (which are the letters EL). The message is SQUIRREL.

27. What is the original message encrypted using the RSA system with $n = 43 \cdot 59$ and $e = 13$ if the encrypted message is 0667 1947 0671? (To decrypt, first find the decryption exponent d which is the inverse of $e = 13$ modulo $42 \cdot 58$.)

27. This problem requires a great amount of calculation. Ideally, one should do it using a computer algebra package, such as *Mathematica* or *Maple*. Let us follow the procedure outlined in Example 9. It was computed there that the inverse of $e = 13$ modulo $n = 43 \cdot 59$ is $d = 937$. We need to compute $0667^{937} \ \mathbf{mod}\ 2537 = 1808$, $1947^{937} \ \mathbf{mod}\ 2537 = 1121$, and $0671^{937} \ \mathbf{mod}\ 2537 = 0417$. (These calculations can in principle be done with a calculator, using the fast modular exponentiation algorithm, but it would probably take the better part of an hour and be prone to transcription errors.) Thus the original message is $1808 \ 1121 \ 0417$, which is easily translated into letters as SILVER.

***28.** Suppose that (n, e) is an RSA encryption key, with $n = pq$ where p and q are large primes and $\gcd(e, (p-1)(q-1)) = 1$. Furthermore, suppose that d is an inverse of e modulo $(p-1)(q-1)$. Suppose that $C \equiv M^e \pmod{pq}$. In the text we showed that RSA decryption, that is, the congruence $C^d \equiv M \pmod{pq}$ holds when $\gcd(M, pq) = 1$. Show that this decryption congruence also holds when $\gcd(M, pq) > 1$. [*Hint:* Use congruences modulo p and modulo q and apply the Chinese remainder theorem.]

28. If $M \equiv 0 \pmod{n}$, then $C \equiv M^e \equiv 0 \pmod{n}$ and so $C^d \equiv 0 \equiv M \pmod{n}$. Otherwise, $\gcd(M,p) = p$ and $\gcd(M,q) = 1$, or $\gcd(M,p) = 1$ and $\gcd(M,q) = q$. By symmetry it suffices to consider the first case, where $M \equiv 0 \pmod{p}$. We have $C^d \equiv (M^e)^d \equiv (0^e)^d \equiv 0 \equiv M \pmod{p}$. As in the case considered in the text, $de = 1 + k(p-1)(q-1)$ for some integer k, so

$$C^d \equiv M^{de} \equiv M^{1+k(p-1)(q-1)} \equiv M \cdot M(^{q-1})^{k(p-1)} \equiv M \cdot 1 \equiv M \pmod{q}$$

by Fermat's little theorem. Thus by the Chinese remainder theorem, $C^d \equiv M \pmod{pq}$.

29. Describe the steps that Alice and Bob follow when they use the Diffie-Hellman key exchange protocol to generate a shared key. Assume that they use the prime $p = 23$ and take $a = 5$, which is a primitive root of 23, and that Alice selects $k_1 = 8$ and Bob selects $k_2 = 5$. (You may want to use some computational aid.)

29. We follow the steps given in the text, with $p = 23$, $a = 5$, $k_1 = 8$, and $k_2 = 5$. Using *Maple*, we verify that 5 is a primitive root modulo 23, by noticing that 5^k as k runs from 0 to 21 produce distinct values (and of course $5^{22} \mathbf{mod}\ 23 = 1$). We find that $5^8 \mathbf{mod}\ 23 = 16$. So in Step (2), Alice sends 16 to Bob. Similarly, in Step (3), Bob sends $5^5 \mathbf{mod}\ 23 = 20$ to Alice. In Step (4) Alice computes $20^8 \mathbf{mod}\ 23 = 6$, and in Step (5) Bob computes $16^5 \mathbf{mod}\ 23 = 6$. These are the same, of course, and thus 6 is the shared key.

30. Describe the steps that Alice and Bob follow when they use the Diffie-Hellman key exchange protocol to generate a shared key. Assume that they use the prime $p = 101$ and take $a = 2$, which is a primitive root of 101, and that Alice selects $k_1 = 7$ and Bob selects $k_2 = 9$. (You may want to use some computational aid.)

30. We follow the steps given in the text, with $p = 101$, $a = 2$, $k_1 = 7$, and $k_2 = 9$. Using *Maple*, we verify that 2 is a primitive root modulo 101, by noticing that 2^k as k runs from 0 to 99 produce distinct values (and of course $2^{100} \mathbf{mod}\ 101 = 1$). We find that $2^7 \mathbf{mod}\ 101 = 27$. So in Step (2), Alice sends 27 to Bob. Similarly, in Step (3), Bob sends $2^9 \mathbf{mod}\ 101 = 7$ to Alice. In Step (4) Alice computes $7^7 \mathbf{mod}\ 101 = 90$, and in Step (5) Bob computes $27^9 \mathbf{mod}\ 101 = 90$. These are the same, of course, and thus 90 is the shared key.

In Exercises 31–32 suppose that Alice and Bob have these public keys and corresponding private keys: $(n_{\text{Alice}}, e_{\text{Alice}}) = (2867, 7) = (61 \cdot 47, 7)$, $d_{\text{Alice}} = 1183$ and $(n_{\text{Bob}}, e_{\text{Bob}}) = (3127, 21) = (59 \cdot 53, 21)$, $d_{\text{Bob}} = 1149$. First express your answers without carrying out the calculations. Then, using a computational aid, if available, perform the calculation to get the numerical answers.

31. Alice wants to send to all her friends, including Bob, the message "SELL EVERYTHING" so that he knows that she sent it. What should she send to her friends, assuming she signs the message using the RSA cryptosystem.

31. See Example 10 for the procedure. First Alice translates her message into numbers: 1804 1111 0421 0417 2419 0708 1306. She then applies her decryption transformation sending each block x to x^{1183} **mod** 2867. (We should verify with *Maple* that $7 \cdot 1183$ **mod** $(60 \cdot 46) = 1$.) Using *Maple*, we see that the blocks become 1804^{1183} **mod** $2867 = 2186$, 1111^{1183} **mod** $2867 = 2087$, 0421^{1183} **mod** $2867 = 1279$, 0417^{1183} **mod** $2867 = 1251$, 2419^{1183} **mod** $2867 = 0326$, 0708^{1183} **mod** $2867 = 0816$, and 1306^{1183} **mod** $2867 = 1948$. If her friends apply Alice's encryption transformation to 2186 2087 1279 1251 0326 0816 1948, they will obtain the numbers of her original message.

32. Alice wants to send to Bob the message "BUY NOW" so that he knows that she sent it and so that only Bob can read it. What should she send to Bob, assuming she signs the message and then encrypts it using Bob's public key?

32. When broken into blocks and translated into numbers the message is 0120 2413 1422. Alice applies her decryption transformation $D_{(2867,7)}(x) = x^{1183}$ **mod** 2867 to each block, which we compute with a CAS to give 1665 1728 2123. Next she applies Bob's encryption transformation $E_{(3127,21)}(x) = x^{21}$ **mod** 3127 to each block, which we compute with a CAS to give 2806 1327 0412. She sends that to Bob. Only Bob can read it, which he does by first applying his decryption transformation $D_{(3127,21)}(x) = x^{1149}$ **mod** 3127 to each block, recovering 1665 1728 2123, and then applying Alice's encryption transformation $E_{(2867,7)}(x) = x^7$ **mod** 2867 to each of these blocks, recovering the original 0120 2413 1422, BUY NOW.

33. We describe a basic key exchange protocol using private key cryptography upon which more sophisticated protocols for key exchange are based. Encryption within the protocol is done using a private key cryptosystem (such as AES) that is considered secure. The protocol involves three parties, Alice and Bob, who wish to exchange a key, and a trusted third party Cathy. Assume that Alice has a secret key k_{Alice} that only she and Cathy know, and Bob has a secret key k_{Bob} which only he and Cathy know. The protocol has three steps:

(i) Alice sends the trusted third party Cathy the message "request a shared key with Bob" encrypted using Alice's key k_{Alice}.

(ii) Cathy sends back to Alice a key $k_{\text{Alice,Bob}}$, which she generates, encrypted using the key k_{Alice}, followed by this same key $k_{\text{Alice,Bob}}$, encrypted using Bob's key, k_{Bob}.

(iii) Alice sends to Bob the key $k_{\text{Alice,Bob}}$ encrypted using k_{Bob}, known only to Bob and to Cathy.

Explain why this protocol allows Alice and Bob to share the secret key $k_{\text{Alice,Bob}}$, known only to them and to Cathy.

33. Cathy knows the shared key $k_{\text{Alice,Bob}}$, but because she transmitted it to Alice encrypted, no one else knows it at the time Alice receives it. Alice can decrypt the first part of Cathy's message to find out what the key is. When Alice sends the second part of Cathy's message, which consists of $k_{\text{Alice,Bob}}$ encrypted with Bob's key, on to Bob, Bob can decrypt it to find the shared key, but it remains hidden from everyone else.

---

18. a) What is the difference between a public key and a private key cryptosystem?

b) Explain why using shift ciphers is a private key system.

c) Explain why the RSA cryptosystem is a public key system.

18. a) See p. 298.

b) The amount of shift, k, is kept secret. It is needed both to encode and to decode messages.

c) Although the key for decoding, d, is kept secret, the keys for encoding, n and e, are published.

---

48. Use the autokey cipher to encrypt the message NOW IS THE TIME TO DECIDE (ignoring spaces) using

a) the keystream with seed X followed by letters of the plaintext.

b) the keystream with seed X followed by letters of the ciphertext.

48. **a)** The seed is 23 (X); adding this mod 26 to the first character of the plaintext, 13 (N), gives 10, which is K. Therefore the first character of the ciphertext is K. The next character of the keystream is the aforementioned 13 (N); add this to O (14) to get 1 (B), so the next character of the ciphertext is B. We continue in this manner, producing the encrypted message KBK A LAL XBUQ XH RHGKLH.

b) Again the seed is 23 (X); adding this mod 26 to the first character of the plaintext, 13 (N), gives 10, which is K. Therefore the first character of the ciphertext is K. The next character of the keystream is the aforementioned K (10); add this to O (14) to get 24 (Y), so the next character of the ciphertext is Y. We continue in this manner, producing the encrypted message KYU CU NUY RZLP IW ZDFNQU.

---

49. Use the autokey cipher to encrypt the message THE DREAM OF REASON (ignoring spaces) using

a) the keystream with seed X followed by letters of the plaintext.

b) the keystream with seed X followed by letters of the ciphertext.

49. **a)** The seed is 23 (X); adding this to the first character of the plaintext, 19 (T), gives 16, which is Q. Therefore the first character of the ciphertext is Q. The next character of the keystream is the aforementioned T (19); add this to H (7) to get 0 (A), so the next character of the ciphertext is A. We continue in this manner, producing the encrypted message QAL HUVEM AT WVESGB.