Math 55—Fall 2025—Haiman
Homework 7

Problems from Rosen

Section 4.6

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 in Example 8.

Answer: Use A–Z $\mapsto$ 00–25, space $\mapsto$ 26; group in pairs to form four–digit numbers.
AT $\to 00\,19 \Rightarrow m_1 = 0019 = 19$, TA $\to 19\,00 \Rightarrow m_2 = 1900$, CK $\to 02\,10 \Rightarrow m_3 = 0210 = 210$.
With $n = 43 \cdot 59 = 2537$ and $e = 13$, compute $c_i \equiv m_i^e \pmod{n}$:

$$c_1 = 19^{13} \equiv 2299, \qquad c_2 = 1900^{13} \equiv 1317, \qquad c_3 = 210^{13} \equiv 2117 \pmod{2537}.$$

Thus the ciphertext is $\boxed{2299\ 1317\ 2117}$.

26. Modified: Use the same $n = 53 \cdot 61$ as in the problem, but take $e = 253$ and decrypt the ciphertext 2642 3218 2887 1068.

Answer: $n = 53 \cdot 61 = 3233$, $\varphi(n) = 52 \cdot 60 = 3120$. Find $d \equiv e^{-1} \pmod{\varphi(n)}$: since $253 \cdot 37 = 9361 \equiv 1 \pmod{3120}$, we have $d = 37$. Decrypt $m \equiv c^{\,d} \pmod{n}$:

c	$m = c^{37} \pmod{3233}$
2642	0614
3218	2601
2887	0400
1068	1718

Decode each block into two letters (A–Z 00–25, space 26):

$$06\,14 \to \texttt{GO}, \quad 26\,01 \to \texttt{ B}, \quad 04\,00 \to \texttt{E }, \quad 17\,18 \to \texttt{RS}.$$

Hence plaintext = $\boxed{\texttt{GO BEARS}}$.

*28. Suppose (n, e) is an RSA key with $n = pq$ and $d \equiv e^{-1} \pmod{(p-1)(q-1)}$. If $C \equiv M^e \pmod{pq}$, show that $C^d \equiv M \pmod{pq}$ *even when* $\gcd(M, pq) > 1$.

Answer: Work modulo p and q separately. Because $ed \equiv 1 \pmod{p-1}$, write $ed = 1 + k(p-1)$. Then

$$C^d \equiv (M^e)^d \equiv M^{ed} \equiv M^{1+k(p-1)} \equiv M\,(M^{p-1})^k \pmod{p}.$$

If $p \nmid M$, then $M^{p-1} \equiv 1$ by Fermat, so $C^d \equiv M \pmod{p}$. If $p \mid M$, then both sides are $\equiv 0 \pmod{p}$, so again $C^d \equiv M \pmod{p}$. The same argument holds mod q. By CRT, $C^d \equiv M \pmod{pq}$ for all M, regardless of $\gcd(M, pq)$.

30. Describe the steps when Alice and Bob run Diffie–Hellman with $p = 101$, primitive root $a = 2$, Alice's secret $k_1 = 7$, Bob's secret $k_2 = 9$. Find the shared key.

Answer: Public base and prime: $a = 2$, $p = 101$.
Alice sends $A \equiv a^{k_1} = 2^7 \equiv 27 \pmod{101}$. Bob sends $B \equiv a^{k_2} = 2^9 \equiv 7 \pmod{101}$.
Shared key:

$$K \equiv B^{k_1} = 7^7 \equiv 90 \pmod{101} \quad (\text{equivalently } K \equiv A^{k_2} = 27^9 \equiv 90).$$

(Check: $7^2 = 49$, $7^4 \equiv 78$, $7^7 = 78 \cdot 49 \cdot 7 \equiv 90$.) Thus $\boxed{K = 90}$.

32. In Exercises 31–32 suppose Alice and Bob have these public keys and corresponding private keys:

$$(n_{\text{Alice}}, e_{\text{Alice}}) = (2867, 7), \quad d_{\text{Alice}} = 1183, \qquad (n_{\text{Bob}}, e_{\text{Bob}}) = (3127, 21), \quad d_{\text{Bob}} = 1149.$$

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?

Answer:

1. **Encode the message.**
   Using the encoding A–Z $\mapsto$ 00–25 and space $\mapsto$ 26, we have:

$$\texttt{B} = 01, \quad \texttt{U} = 20, \quad \texttt{Y} = 24, \quad \texttt{(space)} = 26, \quad \texttt{N} = 13, \quad \texttt{O} = 14, \quad \texttt{W} = 22.$$

   Grouping into pairs gives:

$$m_1 = 0120, \quad m_2 = 2426, \quad m_3 = 1314, \quad m_4 = 2223.$$

2. **Sign each block with Alice's private key.**
   For each block, compute

$$s_i \equiv m_i^{d_{\text{Alice}}} \pmod{n_{\text{Alice}}}, \qquad i = 1, 2, 3, 4.$$

   This produces Alice's digital signature for each block.

3. **Encrypt each signed block with Bob's public key.**
   Each block is then encrypted as:

$$c_i \equiv s_i^{e_{\text{Bob}}} \pmod{n_{\text{Bob}}}, \qquad i = 1, 2, 3, 4.$$

   The ciphertext sent to Bob is (c_1, c_2, c_3, c_4).

4. **Numerical computation.**
   Using $d_{\text{Alice}} = 1183$, $n_{\text{Alice}} = 2867$, $e_{\text{Bob}} = 21$, and $n_{\text{Bob}} = 3127$:

$$(s_1, s_2, s_3, s_4) = (1665,\ 352,\ 1655,\ 2359),$$

   and

$$(c_1, c_2, c_3, c_4) = (2806,\ 298,\ 654,\ 2300).$$

   Therefore, Alice should send the ciphertext blocks:

$$\boxed{2806\ 298\ 654\ 2300.}$$

5. **Verification by Bob.**
   Bob decrypts each block using his private key $d_{\text{Bob}} = 1149$ to recover the signatures s_i, then checks that

$$s_i^{e_{\text{Alice}}} \equiv m_i \pmod{n_{\text{Alice}}}.$$

   Successful verification confirms that the message was signed by Alice and can be read only by Bob.

Additional problems

1. Pollard's ρ factoring algorithm: factor $n = 7081$. Show your steps.

   Answer: Use $f(x) = x^2 + 1 \pmod{n}$, start $x = y = 2$. Iterate $x \leftarrow f(x)$, $y \leftarrow f(f(y))$, $d = \gcd(|x - y|, n)$.

iter	x	y	$d = \gcd(\lvert x - y\rvert, 7081)$
1	$f(2) = 5$	$f(f(2)) = f(5) = 26$	1
2	$f(5) = 26$	$f(f(26)) = f(677) = 7079$	1
3	$f(26) = 677$	$f(f(7079)) = f(5146) = 7079$	**97**

   We obtain a nontrivial factor $d = 97$. Then $7081/97 = 73$. Hence

$$\boxed{7081 = 73 \cdot 97}.$$

2(a). Show that if $a^2 \equiv b^2 \pmod{n}$ with $a \not\equiv \pm b \pmod{n}$, then $\gcd(a - b, n)$ and $\gcd(a + b, n)$ are nontrivial factors of n.

   Answer: From $a^2 \equiv b^2 \pmod{n}$ we have $n \mid (a-b)(a+b)$. Let $d_1 = \gcd(a-b, n)$, $d_2 = \gcd(a+b, n)$. If $a \not\equiv \pm b \pmod{n}$, then $1 < d_1 < n$ and $1 < d_2 < n$ (otherwise $a \equiv b$ or $a \equiv -b$). Thus d_1, d_2 are nontrivial factors of n. □

2(b). Use part (a) (Fermat's method) to factor $n = 6893$ by trying integers $a > \sqrt{n}$ until $a^2 - n$ is a perfect square.

   Answer: $\sqrt{6893} \approx 82.99 \Rightarrow a = 83, 84, 85, 86, 87, \ldots$

a	$a^2 - 6893$
83	-4 (skip)
84	$7056 - 6893 = 163$
85	$7225 - 6893 = 332$
86	$7396 - 6893 = 503$
87	$7569 - 6893 = \mathbf{676} = 26^2$

   Thus $a = 87$, $b = 26$, and $a^2 - b^2 = (a - b)(a + b) = 6893$. Hence

$$\boxed{6893 = (87 - 26)(87 + 26) = 61 \cdot 113}.$$