CMSC 414: HW 2 Solution and Grading

---

1. (text 3.8) Why is a DES weak key its own inverse? (Hint: DES encryption and decryption are the same once the per-round keys are generated.)

For a DES weak key, each of C_0 and D_0 is equal to all ones or all zeros. Each C_i is a permutation of C_0, so each C_i equals C_0. Each D_i is a permutation of D_0, so each D_i equals D_0. K_i depends only on C_i and D_i, so all K_i's are equal. So the sequence $K_1, K_2, \cdots, K_{16}$ is the same as the sequence $K_{16}, K_{15}, \cdots, K_1$. So the encryption operation is the same as the decryption operation (from the hint).

Explanation of the hint: In case the hint is not clear, here are more details.

DES_encryption {
  initial permutation to get $L_0|R_0$ from data block
  for n=1, 2, ⋯, 16 do $L_n|R_n := E_n(K_n, L_{n-1}|R_{n-1})$,
    where E_n denotes the computation of encryption round n.
  swap left and right halves, yielding $R_{16}|L_{16}$
  inverse of initial permutation, yielding cipher block
}

DES_decryption {
  initial permutation of cipher block, yielding $R_{16}|L_{16}$
  for n = 16, 15, ⋯, 1 do $R_{n-1}|L_{n-1} := D_n(K_n, R_n|L_n)$,
    where D_n denotes the computation of decryption round n.
  swap left and right halves, yielding $L_0|R_0$
  inverse of initial permutation, yielding data block.
}

Section 3.3.4 explains that decryption round n is identical to encryption round n with L_n and R_n swapped, i.e., $D_n(K_n, R_n|L_n)$ equals $E_n(K_n, L_n|R_n)$. Substituting this in DES_decryption, we see that the only difference between encryption and decryption is that the K_n's are used in the opposite order. So there is no difference if all the K_i's are the same.

---

2. (text 5.1) Would it be reasonable to compute an RSA signature on a long message m by signing m mod-n (i.e., using $(m \text{ mod-} n)^d \text{ mod-} n$ as the signature).

No. Recall that RSA restricts the message to be signed to be smaller than n.

If m is larger than n, then message m and message (m mod-n) would have the same signature. So it would be easy to generate different messages that have the same signature.

---

3. (text 5.6) Why do MD4, MD5, and SHA-1 require padding of messages that are already a multiple of 512-bits?

Otherwise it would be easiy to find two messages with the same hash. Let M' be any message that is not a multiple of 512 bits. Let M be M' padded as in MD4, so M is a multiple of 512 bits. If no padding is used for M (because it is a multiple of 512 bits) then MD4(M) would be the same as MD4(M').

---

4. (text 6.3) In RSA, is it possible for more than one *d* to work with a given *e, p,* and *q*?

Because d is the multiplicative inverse of e mod-$(p-1)\cdot(q-1)$, it is unique modulo $(p-1)\cdot(q-1)$. [Recall e has a multiplicative inverse mod $(p-1)\cdot(q-1)$ iff e is relatively prime to $(p-1)\cdot(q-1)$. So multiplying the elements of $Z_{(p-1)\cdot(q-1)}$ by e results in a permutation of $Z_{(p-1)\cdot(q-1)}$, so there is only one element in $Z_{(p-1)\cdot(q-1)}$ which yields 1 when multiplied by e.]

---

5. (text 6.8) Given your RSA signature on m_1 and m_2, how can one compute your signature on $m_1^j\cdot m_2^k$ for any positive integers j and k.

Let s_1 be the signature of m_1, i.e., $s_1 = m_1^d$ mod-n.
Let s_2 be the signature of m_2, i.e., $s_2 = m_2^d$ mod-n.
Signature(m_1^j) = s_1^j mod-n [because $(m_1^j)^d$ mod-n = $(m_1^d)^j$ mod-n].
Signature(m_1^{-1}) = s_1^{-1} mod-n [because $(m_1^{-1})^d$ mod-n = $(m_1^d)^{-1}$ mod-n], assuming m_1^{-1} exists.
Signature($m_1\cdot m_2$) = $s_1\cdot s_2$ mod-n [because $(m_1\cdot m_2)^d$ mod-n = $(m_1^d)\cdot(m_2^d)$ mod-n].
Signature($m_1^j\cdot m_2^k$) = $s_1^j\cdot s_2^k$ mod-n [from above].

---

6. Using the efficient algorithm, compute 131^{25} mod-15.

$25 = (11001)_2$ [25 = 16 + 8 + 1]
$131^{(1)}$ mod-15 = 11
$131^{(10)}$ mod-15 = 11·11 mod-15 = 121 mod-15 = 1
$131^{(11)}$ mod-15 = 1·11 mod-15 = 11 mod-15 = 11
$131^{(110)}$ mod-15 = 11·11 mod-15 = 121 mod-15 = 1
$131^{(1100)}$ mod-15 = 1·1 mod-15 = 1
$131^{(11000)}$ mod-15 = 1·1 mod-15 = 1
$131^{(11001)}$ mod-15 = 1·11 mod-15 = 11
So 131^{25} mod-15 = 11

---

7. (text 7.1) If m and n are two positive integers, show that m/gcd(m,n) and n/gcd(m,n) are relatively prime.

By Euclid's algorithm, there exist integers u and v such that $u \cdot m + v \cdot n = \gcd(m,n)$.
Dividing both sides by gcd(m,n) gives $u \cdot (m/\gcd(m,n)) + v \cdot (n/\gcd(m,n)) = 1$.
So by Euclid algorithm, m/gcd(m,n) and n/gcd(m,n) are relatively prime (note that both are integers by definition of gcd).

---

8. (text 7.10) If $n = p_1^{a1} \cdot p_2^{a2} \cdots p_k^{ak}$ where p_i is prime, what is $\phi(n)$.

   We have already established the following:
   - $\phi(p^a) = (p-1) \cdot p^{a-1}$ for p prime and $a > 0$
   - $\phi(p \cdot q) = \phi(p) \cdot \phi(q)$ for p and q relatively prime

   We also have that if p_1, p_2, ⋯, p_n, q are distinct primes, then $(p_1^{a1} \cdot p_2^{a2} \cdots p_n^{an})$ and q^b are relatively prime.

   Hence by induction
   $$\phi(p_1^{a1} \cdot p_2^{a2} \cdots p_k^{ak}) = (p_1-1) \cdot p_1^{a1-1} \cdot (p_2-1) \cdot p_2^{a2-1} \cdots (p_k-1) \cdot p_k^{ak-1}$$

---

9. Find all the square roots mod-15 of 1, i.e., every x in Z_{15} such that $x \cdot x$ mod-15 = 1.

1^2 mod-15 = 1
2^2 mod-15 = 4
3^2 mod-15 = 9
4^2 mod-15 = 16 mod-15 = 1
5^2 mod-15 = 25 mod-15 = 10
6^2 mod-15 = 36 mod-15 = 6
7^2 mod-15 = 49 mod-15 = 3
8^2 mod-15 = 64 mod-15 = 4
9^2 mod-15 = 81 mod-15 = 6
10^2 mod-15 = 100 mod-15 = 10
11^2 mod-15 = 121 mod-15 = 1
12^2 mod-15 = 144 mod-15 = 9
13^2 mod-15 = 169 mod-15 = 4
14^2 mod-15 = 196 mod-15 = 1
So the square roots mod-15 of 1 are {1, 4, 11, 14}

[Check: $15 = 2^0 \cdot 3 \cdot 5$. So the formula at the end of section 7.5 tells us that there are 2^2 square roots mod-15 of 1.]

---

10. Find all the square roots mod-24 of 1.

Before going through the numbers in Z_{24}, let's use the formula at the end of section 7.5 to see how many square roots there are. $24 = 2\cdot2\cdot2\cdot3 = 2^3\cdot3$, so there are 2^3 square roots.

- $1\cdot1$ mod-24 = 1
- $23\cdot23$ mod-24 = 529 mod-24 = 1
- $5\cdot5$ mod-24 = 25 mod-24 = 1.
- $7\cdot7$ mod-24 = 49 mod-24 = 1.
- $11\cdot11$ mod-24 = 121 mod-24 = 1
- $13\cdot13$ mod-24 = 169 mod-24 = 1
- $17\cdot17$ mod-24 = 289 mod-24 = 1
- $19\cdot19$ mod-24 = 361 mod-24 = 1

So the roots are 1, 5, 7, 11, 13, 17, 19, 23.

[Can one restrict the search to Z_n*?
 Is $1\cdot1$ mod-n = 1 for any n?
 Is $(n-1)\cdot(n-1)$ mod-n = 1 for any n?]

---

11. Given positive integers z_1, z_2, z_3, x_1, x_2, x_3, such that z_1, z_2, z_3 are relatively prime, obtain a formula that yields a number x in $Z_{z1\cdot z2\cdot z3}$ such that
 x mod-$z_1 = x_1$
 x mod-$z_2 = x_2$
 x mod-$z_3 = x_3$

The Chinese remainder theorem shows us that there is exactly one such x and how to compute it.

Applying the CRT to z_1 and z_2 yields the following:

- Let a and b satisfy $1 = a\cdot z_1 + b\cdot z_2$ [a and b can be computed by Euclid(z_1, z_2)]
- Let p = [$x_2\cdot a\cdot z_1 + x_1\cdot b\cdot z_2$] mod $z_1\cdot z_2$
- Then p mod-$z_1 = x_1$ and p mod-$z_2 = x_2$

Applying the CRT to $z_1\cdot z_2$ and z_3 yields the following:

- Let c and d satisfy $1 = c\cdot(z_1\cdot z_2) + d\cdot z_3$ [c and d can be computed by Euclid($z_1\cdot z_2$, z_3)]
- Let q = [$p\cdot c\cdot(z_1\cdot z_2) + x_3\cdot d\cdot z_3$] mod $z_1\cdot z_2\cdot z_3$
- Then q mod-$(z_1\cdot z_2)$ = p and q mod-$z_3 = x_3$

Thus q is the number x we want.

In summary, x = [$p\cdot c\cdot(z_1\cdot z_2) + x_3\cdot d\cdot z_3$] mod $z_1\cdot z_2\cdot z_3$ where

- p = [$x_2\cdot a\cdot z_1 + x_1\cdot b\cdot z_2$] mod $z_1\cdot z_2$
- c and d satisfy $1 = c\cdot(z_1\cdot z_2) + d\cdot z_3$
- a and b satisfy $1 = a\cdot z_1 + b\cdot z_2$
