Problem 12.2 from the textbook:

Answer:

The CBC mode with an IV of 0 and plaintext blocks D1, D2, . . ., Dn and 64-bit CFB mode with IV = D1 and plaintext blocks D2, D3, . . ., Dn yield the same result.

Problem 12.3 from textbook:

Answer:

We use the definition from Section 12.6. For a one-block message, the MAC using CBC-MAC is T = E(K, X), where K is the key and X is the message block. Now consider the two-block message in which the first block is X and the second block is X $\oplus$ T. Then the MAC is

E(K, [T $\oplus$ (X $\oplus$ T)]) = E(K, X) = T.

Problem 13.8 from the textbook:
Answer:

a. The receiver validates the digital signature by ensuring that the first 56-bit key in the signature will encipher validation parameter u1 into E(k1, u1) if the first bit of M is 0, or that it will encipher U1 into E(K1, U1) if the first bit of M is 1; the second 56-bit key in the signature will encipher validation parameter u2 into E(k2, u2) if the second bit of M is 0, or it will encipher U2 into E(K2, U2) if the second bit of M is 1,; and so on.

b. Only the sender, who knows the private values of ki and Ki and who originally creates vi and Vi from ui and Ui can disclose a key to the receiver. An opponent would have to discover the value of the secret keys from the plaintext-ciphertext pairs of the public key, which was computationally infeasible at the time that 56-bit keys were considered secure.

c. This is a one-time system, because half of the keys are revealed the first time.

d. A separate key must be included in the signature for each bit of the message resulting in a huge digital signature.

Problem 4: The following two sub problems involve Fermat's Theorem.

(a) Using Fermat's Theorem, find $3^{201} \bmod 11$.
(b) Using Fermat's Theorem, find a number x between 0 and 28 with x^{85} congruent to 6 modulo 29. (you should not use any brute-force searching)

Answer:

(a) Fermat's Theorem states that if p is prime and a is a positive integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$. Therefore $3^{10} \equiv 1 \pmod{11}$. Therefore $3^{201} = (3^{10})^{20} \times 3 \equiv 3 \pmod{11}$.

(b) Since p-1=28, 85=28×3+1, and $x^{28} \equiv 1 \pmod{29}$, so we have $x^{85} = (x^{28})^{3} \times x \equiv 6 \pmod{29}$. Thus, x=6.

Problem 5: The following two sub problems involve Euler's Theorem.

(a) Using Euler's Theorem, find a number a between 0 and 9 such that a is congruent to $7^{1000} \bmod 10$. (note: this is the same as the last digit of the decimal expansion of 7^{1000})

(b) Using Euler's Theorem, find a number x between 0 and 28 with x^{85} congruent to 6 modulo 35. (you should not use any brute-force searching)

Answer:

Euler's Theorem states that if n and a are coprime positive integers, then

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

(a) Since $\varphi(10) = 4$, $7^{1000} = 7^{4*250} \equiv 7^0 \pmod{10} = 1$.

(b) Since $\varphi(35) = 4 * 6 = 24$, and 85= 24*3+13. This means $x^{13} \equiv 6 \pmod{35}$. If we mod 7 on both sides of the above equation, $x^{13} = x^{7*2-1} \equiv x^{-1} \pmod{7} \equiv 6 \pmod{7}$. This means x is the multiplicative inverse of 6 mod 7, which gives x=6.

Alternative method: mod 13 on both sides of the above.

Problem 6: Suppose Fred sees your RSA signature on m_1 and on m_2 (i.e. he sees $m_1^d \bmod n$ and $m_2^d \bmod n$). How does he compute the signature on each of these messages: $m_1^j \bmod n$ (for positive integer j), $m_1^{-1} \bmod n$, $m_1 \cdot m_2 \bmod n$, and in general $m_1^j \cdot m_2^k \bmod n$ (for arbitrary integers j and k)?

Answer:

$(m_1^j)^d \bmod n = (m_1^d)^j \bmod n$, so to compute your signature on $m_1^j \bmod n$, Fred just raises your signature on m_1 to the jth power, mod n.

$(m_1^{-1})^d \bmod n = (m_1^d)^{-1} \bmod n$, so to compute your signature on $m_1^{-1} \bmod n$, Fred just computes the inverse mod n of your signature on m_1.

$(m_1 \cdot m_2)^d \bmod n = m_1^d \cdot m_2^d \bmod n$, so to computer your signature on $m_1 \cdot m_2 \bmod n$, Fred just multiplies your signature on m_1 by your signature on m_2, mod n.

So for the general case of $m_1^j \cdot m_2^k \bmod n$, Fred gets your signature on $m_1^{\text{sgn } j} \bmode n$ and raises it to the $|j|$th power, mod n, then gets your signature on $m_2^{\text{sgn } k} \bmod n$ and raises it to the $|k|$th power, mod n, and finally multiplies the results together, mod n.

[sgn x= x/|x|]

Problem 7: Alice can send Bob: $E_{pkB}(x||ID_A)$, $Sig_{skA}(E_{pkB}(x||ID_A))$, or

$E_{pkB}(E_{pkB}(x), Sig_{skA}(E_{pkB}(x)))$

Additional problems for 471 students only:

Problem 9.3 from textbook
Answer: 5

Problem 9.8 from textbook
Consider a set of alphabetic characters {A, B, …, Z}. The corresponding integers, representing the position of each alphabetic character in the alphabet, form a set of message block values SM = {0, 1, 2, …, 25}. The set of corresponding ciphertext block values SC = {0^e mod N, 1^e mod N, …, 25^e mod N}, and can be computed by everybody with the knowledge of the public key of Bob. Thus, the most efficient attack against the scheme described in the problem is to compute Me mod N for all possible values of M, then create a look-up table with a ciphertext as an index, and the corresponding plaintext as a value of the appropriate location in the table.

Problem 11.1 from textbook
a. Yes. The XOR function is simply a vertical parity check. If there is an odd number of errors, then there must be at least one column that contains an odd number of errors, and the parity bit for that column will detect the error. Note that the RXOR function also catches all errors caused by an odd number of error bits. Each RXOR bit is a function of a unique "spiral" of bits in the block of data. If there is an odd number of errors, then there must be at least one spiral that contains an odd number of errors, and the parity bit for that spiral will detect the error.

b. No. The checksum will fail to detect an even number of errors when both the XOR and RXOR functions fail. In order for both to fail, the pattern of error bits must be at intersection points between parity spirals and parity columns such that there is an even number of error bits in each parity column and an even number of error bits in each spiral.

c. It is too simple to be used as a secure hash function; finding multiple messages with the same hash function would be too easy.

Additional problems for 571 students only:

Problem 9.18 from textbook.
Answer: Note that, because $Z = r^e mod\ n$, then $r = Z^d mod\ n$. Bob computes:

$$tY\ mod\ n = r^{-1}X^d mod\ n = r^{-1}Z^d C^d mod\ n = C^d mod\ n = \text{M}$$

Problem 11.3 from the textbook:
Answer:

a. It satisfies properties 1 through 3 but not the remaining properties. For example, for property 4, a message consisting of the value h satisfies $H(h) = h$. For property 5, take any message M and add the decimal digit 0 to the sequence; it will have the same hash value.

b. It satisfies properties 1 through 3. Property 4 is also satisfied if n is a large composite number, because taking square roots modulo such an integer n is considered to be infeasible. Properties 5 and 6 are not satisfied because –M will have the same value as M.

c. 229

Problem 12.9 from the textbook:
Answer:

a. The following matrix shows the message for each received 2-bit word.

	Word			
Key	00	01	10	11
1	0	1	—	—
2	1	—	0	—
3	—	0	—	1
4	—	—	1	0

b. The probability that someone can successfully impersonate Alice is 0.5 because only two of the four words are possible as transmitted word under the joint secret key.

c. An opponent Eve who tries to replace a transmitted message by another one will know that only two keys can possibly have been used, but she doesn't know which one. So, the probability of a successful substitution is also 0.5.