Midterm: Part I

Note

This is a closed-book exam. Part I contains five problems, each accounting for 10 points.

Problems

1. Consider the AES algorithm, where the irreducible polynomial modulus is $x^8+x^4+x^3+x+1$.
   (a) What is the result of (1101 1001) $\cdot$ (0000 0110)? Show the steps of your calculation.
   (b) What is the value of $(0110\ 0101)^{-1}$? Show the steps of your calculation.
2. (a) How does three-key triple DES achieve backward compatibility with DES? Please describe all alternatives.
   (b) Why does the encryption algorithm of AES run faster than the decryption algorithm? How is this fact useful?
3. (a) Why are the various modes of operation needed for block ciphers?
   (b) What are the advantages of the Counter (CTR) Mode of Operation for symmetric block ciphers? Please give five of them.
4. What is a hierarchical key control (for key distribution)? How does it operate? What are its advantages?
5. Below is a simple authentication protocol that has been studied in the literature. It relies on a trusted third party C that shares a (distinct) secret key with each principle in the system. The key shared between C and a principle P is denoted K_P. $\{M\}_K$ denotes a message containing the plaintext M encrypted with the key K. A nonce is essentially some information that has never appeared before (at the time when the nonce is generated). Please explain why Q can be certain after step (6) that (assuming there is only one session of this protocol running) it was really P who sent the message "I am P".

$$
\begin{array}{lll}
(1) & P \rightarrow Q & : \text{“I am } P\text{”} \\
(2) & Q & : \text{generate nonce } n \\
(3) & Q \rightarrow P & : n \\
(4) & P \rightarrow Q & : \{n\}_{K_P} \\
(5) & Q \rightarrow C & : \{P, \{n\}_{K_P}\}_{K_Q} \\
(6) & C \rightarrow Q & : \{n\}_{K_Q}
\end{array}
$$

(5 bonus points) The protocol above is in fact incorrect when there can be multiple sessions running simultaneously. Can you find a problematic scenario?

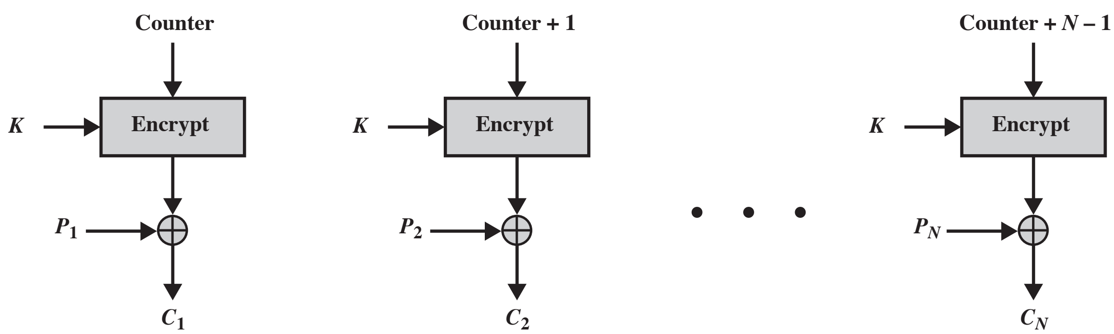
Appendix

- The extended Euclid's algorithm for polynomials is as follows.

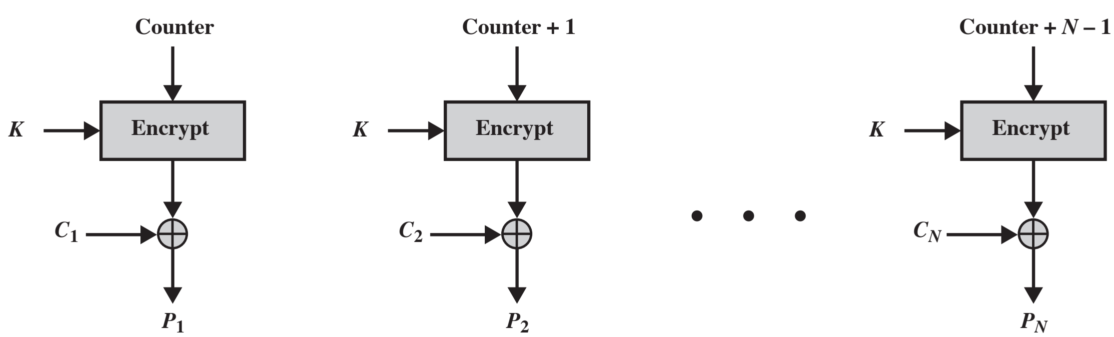
    $EXTENDED\ EUCLID(m(x), b(x))$:

    1. $[A_1(x), A_2(x), A_3(x)] \leftarrow [1, 0, m(x)]; [B_1(x), B_2(x), B_3(x)] \leftarrow [0, 1, b(x)]$
    2. if $B_3(x) = 0$ then return $A_3(x) = \gcd(m(x), b(x))$; no inverse
    3. if $B_3(x) = 1$ then return $A_3(x) = \gcd(m(x), b(x)); B_2(x) = b^{-1}(x) \pmod{m(x)}$
    4. $Q(x) =$ the quotient of $A_3(x)/B_3(x)$
    5. $[T_1(x), T_2(x), T_3(x)] \leftarrow [A_1(x) - Q(x)B_1(x), A_2(x) - Q(x)B_2(x), A_3(x) - Q(x)B_3(x)]$
    6. $[A_1(x), A_2(x), A_3(x)] \leftarrow [B_1(x), B_2(x), B_3(x)]$
    7. $[B_1(x), B_2(x), B_3(x)] \leftarrow [T_1(x), T_2(x), T_3(x)]$
    8. goto 2

- The Counter (CTR) Mode of Operation in picture:



(a) Encryption



(b) Decryption