Family Name:.........................

First Name:...........................

Section:..............................

Security Protocols and Applications
(Part 2/2: CBE)

Final Exam

July 1st, 2008

Duration: 2 hours (for the 2 parts)

This document consists of 6 pages.

Instructions

Electronic devices are *not* allowed.

All printed documents are permitted.

Answers must be written on the exercises sheet.

This exam contains 2 *independent* parts.

This part contains 1 exercise.

Answers can be either in French or English.

Questions of any kind will certainly *not* be answered. Potential errors in these sheets are part of the exam.

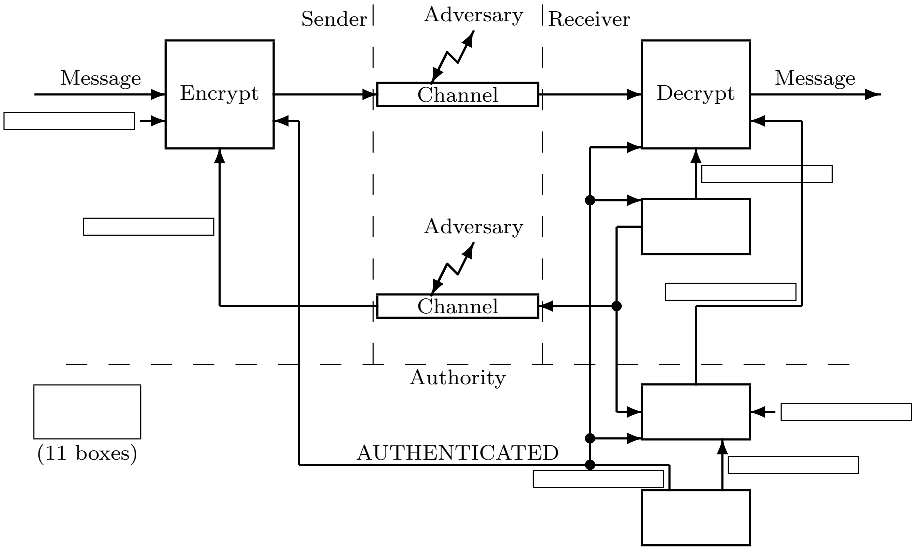
You have to put your full name on the first page of each document and have all pages *stapled*.

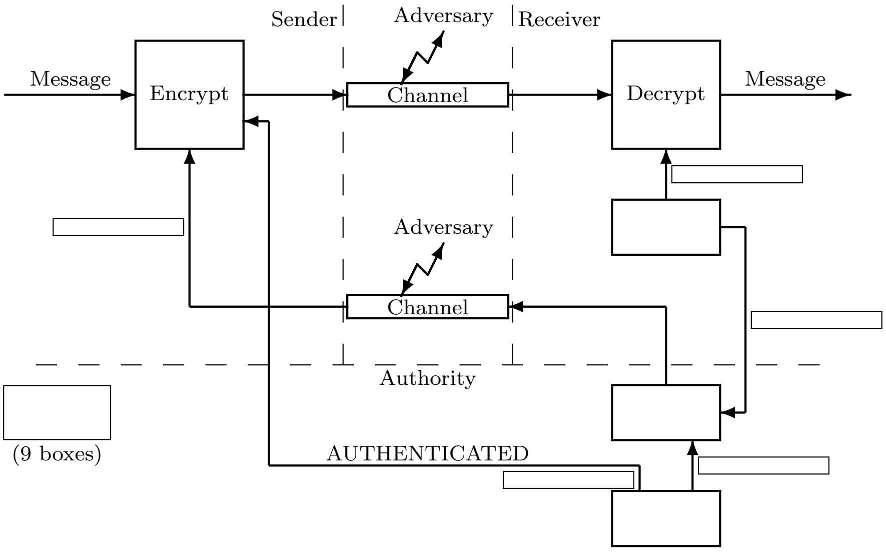
1 Certificate-Based Encryption

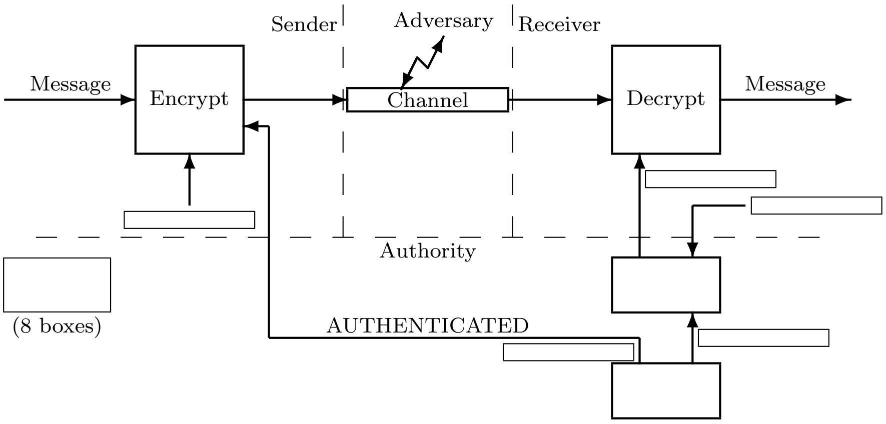
1.1 Preliminaries

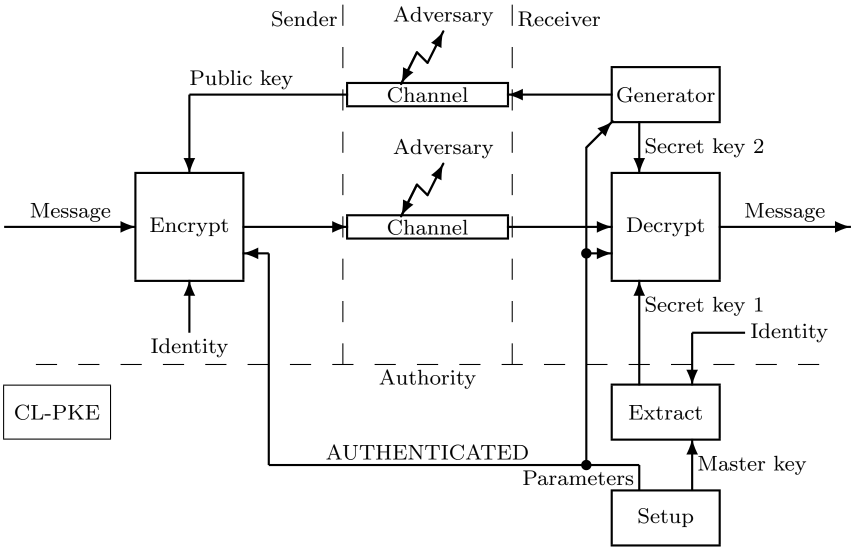
1. The following pictures describe (in a random order) the data flow related to 3 different technologies: Public-Key Infrastructure (PKI), Identity-Based Encryption (IBE), and Certificate-Based Encryption (CBE). Fill the boxes with the name of the algorithms, the name transmitted data, and the name of the technology.

   (A solution example with a fourth technology CL-PKE is given.)









2. What is the advantage of CBE over PKI?

3. What is the advantage of CBE over IBE?

1.2 Case study

We consider a large bank with 10 000 employees having to receive encrypted messages from customers. Encryption is realized using public-key but the public-key authentication to users is critical. We assume that each employee receives on average 50 encrypted emails from different customers every day. Two technologies are being considered: (A) a PKI with Online Certificate Status Protocol (OCSP); and (B) CBE. In both cases, certificates and revocations are managed by a central server denoted CA. In the (A) case, we assume that public keys are valid during 100 days. In the (B) case, these are valid during 1 000 days with an elementary time period of 4 days.

4. Give at least two reasons why a public-key would have to be revoked.

5. How many OCSP queries from customers are made to the CA in case (A) and case (B)?

6. How many new public keys per day the CA has to register in case (A) and case (B) on average?

7. How many certificates per day the CA has to send out in case (A) and case (B) on average?

8. What is the difference between the domain parameters that the CA sets up in case (B) and the CA public key in case (A)?

Any attempt to look at
the content of these pages
before the signal
will be severly punished.

Please be patient.