Chapter 11 | Public-Key Encryption

Tuesday, November 7, 2023 11:44 AM

11.1 Public-Key Encryption—An Overview

Story:

- The introduction of public-key encryption
  marked a revolution in crytpography.
  - Until that time
    cryptographers had relied exclusively on shared
    secret keys
    to achive private communication.
  - Public-key techniques
    in contrast
    enabled parties to communicate privately
    without having agreed on any secret information
    in advance.
  - As we have already noted
    it is quite amazing and counterintuitive that
    this is possible
    it means that two people on opposite sides of a room
    who can only communicate by shouting to each other
    and have no initila secret
    can talk in such a way that
    no one else in the room learns anything about what they are saying.
- In the setting of private key encryption
  two parties agree on a secret key that can be used
  by either party
  for both encryption and decryption
  - Public key encryption is
    assymetric in both these respects
  - On party (the reciever)
    generates a pair of keys (pk, sk)
    called the public key and the private key resp.
  - The public key is used by a sender
    to encrypt a message
    the receiver uses the private key
    to decrypt the resulting ciphertext.
- Since the goal is to avoid the need for
  two parties to meet in advance to agree on any information

how does the sender learn pk?

[ME: Here, the emphasise is that the channel is assumed to ***authenticated*** *and public]*

At an abstract level
this can happen in two ways:

- □ Call the receiver Alice and
- □ the sender Bob

- In the first approach
  when Alice learns that Bob wants t o communicate with here
  She can at that point generate
  pk, sk
  (assuming she hasn't done so already)
  and
  then send pk to Bob in *the clear*.

  Bob can then use pk to encrypt his message.

  We emphasise that the channel between Alice and Bob may
  be public
  but is assumed to be **authenticated**
  meaning that the adversary cannot modify the public key
  sent by Alice to Bob
  (and in particular cannot replace it with its own key)

  See Section 12.7 for a discussion of how public keys can
  be distributed over **unauthenticated channels**.

- An alternative approach
  is for Alice to generate hehr keys (pk, sk) in advance
  independently of any particular sender
  (in fact, at the time of key gnereation
  Alice need not even be aware that
  Bob wants to talk to her
  or even that Bob exists).

  - ○ Alice can widely disseminate her public key pk
    by, say, publicshing it on her webpage
    putting it on her business cards ....

  - ○ Now, anyone who wishes to communicate privately with Alice
    can look up her public key and proceed as above.

  - ○ Note that multple senders can communicate multiple times
    with Alice using the same public key pk for
    encrypting all their communication.

- Note that pk is inherently public—
  and can thus be learned easily by an attacker—in either of the above scenarios.

  In the first case
  an adversary eavsdropping on the communication between
  Alice and bob obtains pk dierrcytl
  in the second case
  an adversary could just as well look up Alic's public key on its own.

  We see that the security of public-key cannot rely on secrecy of pk
  and must rely on secrecy of sk

  It is therefore crucial
  that Alice does not revea her private key
  to anyone
  including the sender Bob.

Comparison to Private-Key Encryption

- Perhaps the most obvious difference
  b/w private and public key encryption is that
  the former assumes *complete secrecey*
  of all cryptograph keys
  whereas the latter requires
  secrecy for only the private key sk.

  - Although this may seem like a minor distinction
    the ramificatinos.