Safe Computing

Data Encryption & Secure Internet Protocols

Safe Computing

Data Encryption & Secure Internet Protocols

- *Encryption* is the process of using an algorithm to convert *plaintext* into *ciphertext*.
  - e.g.: "CAT" ➡ "DBU" via Caesar cipher
    - All letters shifted down the alphabet by the same key (+1)
    - To decrypt, reverse the process
    - All letters shifted up the alphabet (-1)
    - "DBU" ➡ "CAT"

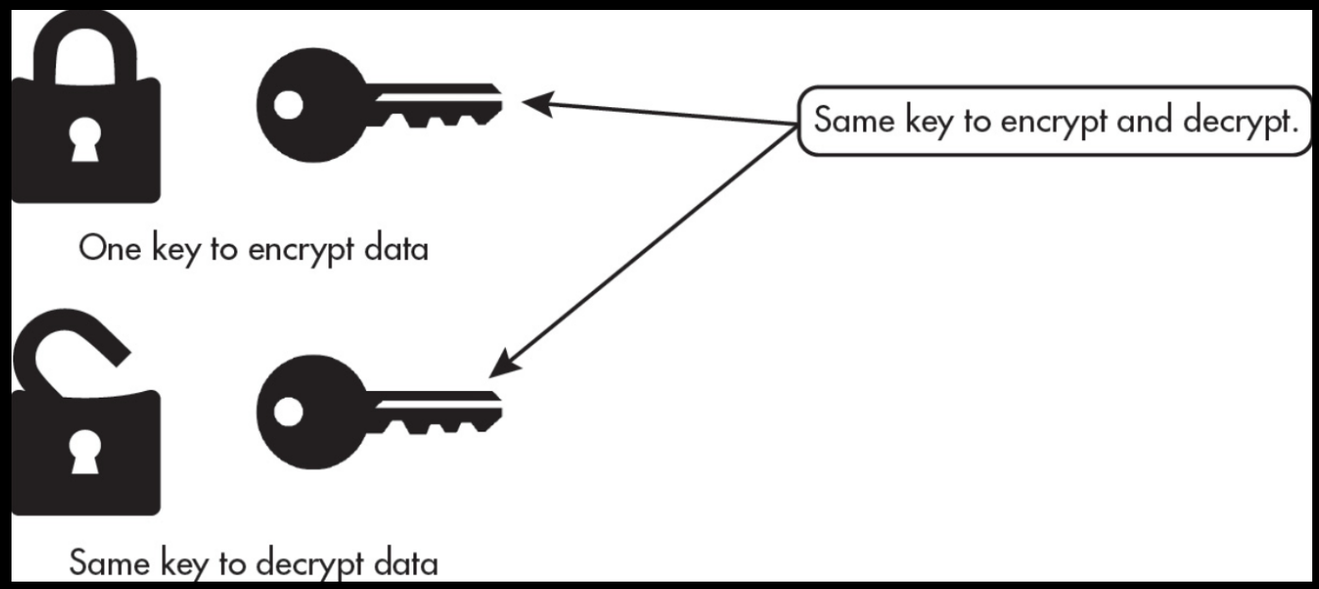
Safe Computing

Data Encryption & Secure Internet Protocols

- *Symmetric key encryption* uses the same key for both encryption and decryption.
  - Key must be agreed upon by sender and receiver in advance.

- This doesn't work well for computers – how can two computers agree upon a key in private in advance?

- They can't... at least, not without something else that happens first.



Safe Computing

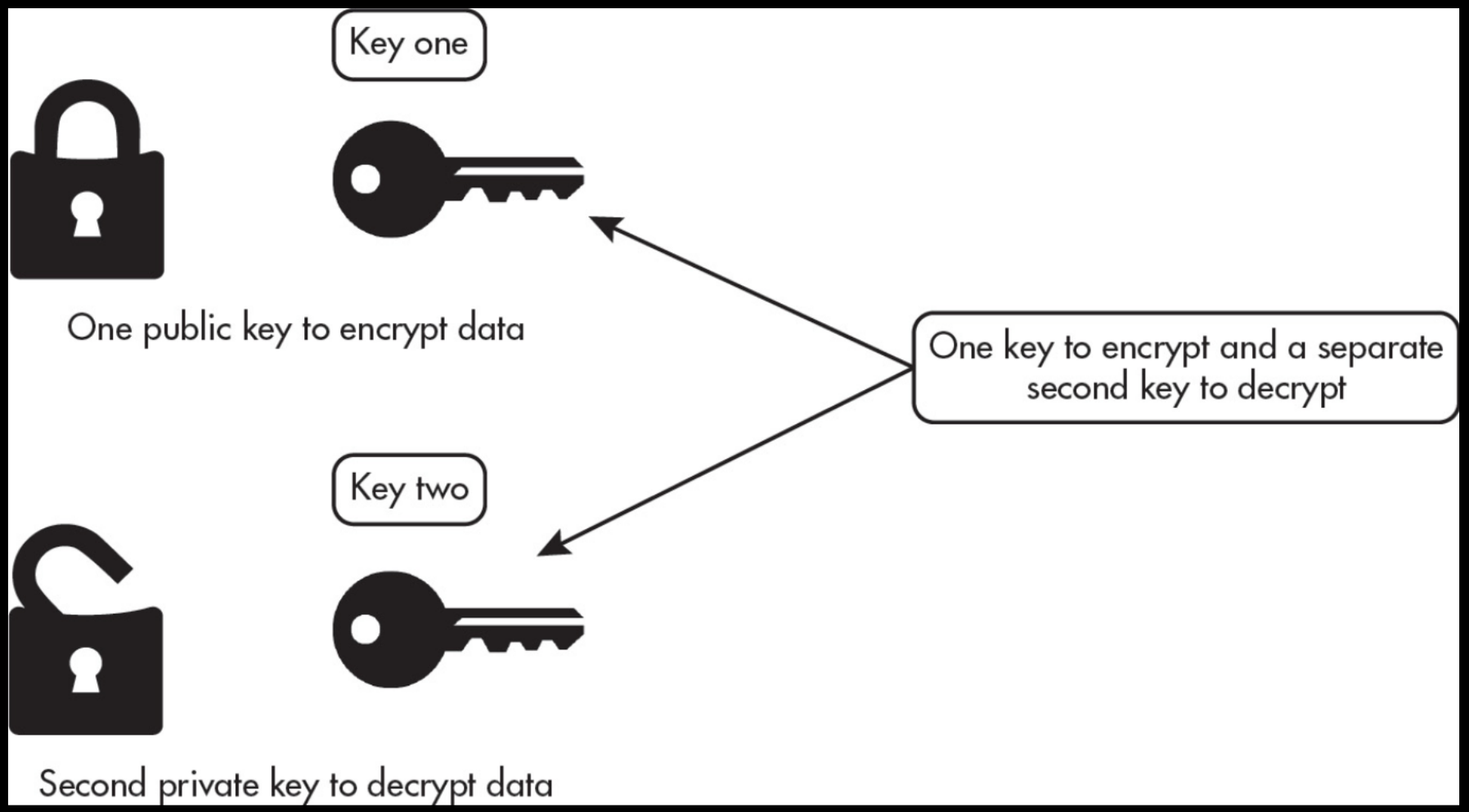
Data Encryption & Secure Internet Protocols

- *Asymmetric key encryption* (also called "public key encryption") uses two keys
    - A *public key* is just that – available to anyone – and is used to encrypt a message
    - However, ciphertext can only be decrypted using the *private key*
        - The private key must be kept secret and is held only by the receiver of a message
    - Do not need to know how public key encryption is implemented but must know how it is used, as described above

Safe Computing

Data Encryption & Secure Internet Protocols

- *Asymmetric key encryption* (also called "public key encryption")



Safe Computing

Data Encryption & Secure Internet Protocols

- Public key encryption is used in SSL (Secure Sockets Layer) and TLS (transport layer security)
  - SSL and TLS enable secure communication on an insecure network
  - But... how do we know that the public key a web server provides is legitimate? That the key delivered by the computer responding at "www.apple.com" was actually issued to Apple, Inc.?
- This works on a "trust model"
  - We trust the web browser (or operating system) we are using
  - Our browser trusts only certain Certificate Authorities (CA's)
  - CA's issue certificates to website operators which includes some amount of identity verification
- Our browser talks directly to a website (CA is not in the middle)
  - Browser checks a website's certificate using information it has from the CA
  - If that check succeeds... communication with website continues

Safe Computing

Data Encryption & Secure Internet Protocols

- Our browser uses asymmetric / public key encryption and certificates to verify identity of a website
    - Once website is trusted, asymmetric encryption used to share a *symmetric encryption key*
        - This symmetric key is used to handle all further communication between our computer and the web server ("secure tunnel")
- Why not just use asymmetric encryption/decryption for *all* communication between our computer and web server?
    - It is slower...
    - Symmetric key encryption/decryption is much faster.

Safe Computing

Data Encryption & Secure Internet Protocols

- Symmetric encryption, asymmetric encryption aka public key encryption, SSL, TLS, certificates, certificate authorities... I've gone cross-eyed! 😭
- What you need to know...
  - The difference between symmetric and asymmetric encryption
  - Larger key lengths mean longer times required to use brute force to decrypt a message when attacker does not know the key
    - Current day computers too slow to do this
  - SSL & TLS use public key encryption
    - Certificate authorities issue digital certificates to certify authenticity of public keys for a given website; system is based on the "trust" model

Safe Computing

Data Encryption & Secure Internet Protocols

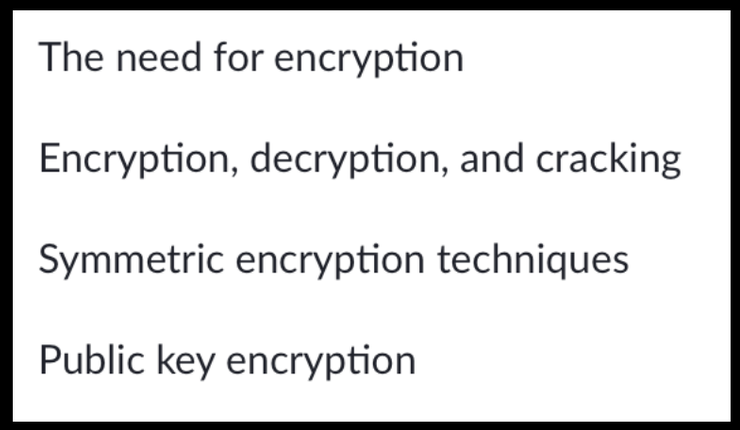
- If you want to know a *bit* more about the steps involved in communication using SSL or TLS... this is pretty good six-minute overview:

- This level of detail is not on the AP CSP exam.
- Understanding this at the implementation level could be an entire course.

Suggested Exercises

Data Encryption & Secure Internet Protocols

- From Khan Academy, finish:
  - Data encryption techniques



  - Secure Internet protocols

- ... and related practice quizzes.
- NOTE: TLS negotiation process is not on AP CSP exam.