Flipped Classroom Session 5: Cryptography

CS-E3130 Information Security, 26.09.2023

1. Symmetric cryptography

a. A collision occurs when a function $f(\cdot)$ applied to two distinct inputs, x and y, results in identical values $f(x) = f(y)$.

1. Do any/all hash functions have collisions? Why/why not?

2. Do any/all block ciphers have collisions (given some fixed key)? Why/why not?

b. An official document contains a signed hash of its contents. Can an attacker forge a document from the same signer using a collision attack, and with a second-preimage attack...

1. If the document contains only data controlled by the agency issuing the document?

2. If the document contains data controlled by the attacker?

c. If a hash preimage attack against a 256-bit hash requires 2^{256} hash computations, then why is cracking as password hash possible with so many fewer computations?

2. Asymmetric cryptography

a. How do public-key encryption and Diffie-Hellman differ in the functionality that they provide?

b. What is the advantage of hybrid encryption over either public-key or symmetric encryption alone?

c. In the exercises, you generated a public/private key pair that was used for SSH authentication. The key pair was generated on your machine, and the public key uploaded to the server.

What would be a disadvantage of instead generating the key pair on the server, and downloading the private key to your local machine?