

## "I don't Know Much About Cryptography - what is a Hash Function?"

One of the main workhorses of modern cryptography are collision resistant hash functions. Given an (almost) arbitrarily long input  $M$ , they produce a fixed-size output  $H(M)$ . Collision resistance means that it is infeasible to find two different inputs  $M$  and  $M'$  with the same hash  $H(M)=H(M')$ . Note that many collisions exist, but it has to be infeasible to actually find even a single collision!

Hash functions are almost omnipresent in today's cryptography, e.g. in digital signatures. Instead of signing a long message  $M$ , you simply sign its hash  $H(M)$ . This is useful and simplifies many issues ... but if  $H(M)$  is identical to  $H(M')$  then the signature is also valid for  $M'$ .

### The Story of Alice and her Boss

Alice has been an intern, working some weeks in Rome at the office of, say, Julius Caesar. Depending on the point of view, the story develops quite differently.

#### Caesar's View

At the day Alice is supposed to leave, Caesar writes a letter of recommendation for Alice -- on paper. The same day, she asks Caesar to digitally sign the letter. For his convenience she presents an electronic copy of the document. Caesar opens the document -- it looks exactly like the original document. So he signs the document.

Months later, Caesar discovers that there has been a breach of secrecy with his French affair files. Will he ever find out who tricked him and how?

#### Alice's View

Being an intern, Alice does not have any access to secret documents. Not enough for her ...

... tricky Alice decides to fool Caesar. Because Caesar is still relying on the widely used MD5 hash function, she implements the attack from Wang and Yu [WY05] to find MD5 collisions. When she receives her letter of recommendation (on paper), she prepares two postscript files with the same MD5 hash:

\* One to display the letter of recommendation, and

\* a second one, an order from Caesar to grant Alice some kind of a security clearance. Now she asks Caesar to sign the letter ... who has no obvious reason to decline.

Due to the hash collision, Caesar's signature for the letter of recommendation is valid for the order, as well. She presents order and digital signature to the person in charge of Caesar's files ... and finally gains access to Caesar's secret documents!