SECURITY (COMP0141):
LAST WEEK → THIS WEEK

INTEGRITY

"system and data have not been improperly altered"

how to:
• know who you're talking to?
• know what data you're getting?

confidentiality

availability

2
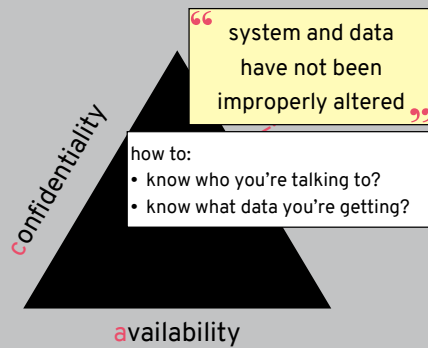
Last week was all about integrity

CRYPTOGRAPHIC PRIMITIVES

—

	setup?	confidentiality/integrity?	fast?
SE	yes	confidentiality	yes
PKE	no*	confidentiality	no
digital signature	no*	integrity	no
MAC	yes	integrity	yes
OWF	no	confidentiality*	no
hash function	no	integrity	yes
AE	yes	both	yes

3

We've seen a lot of cryptography so far, to achieve both confidentiality and integrity

DIGITAL SIGNATURES

—
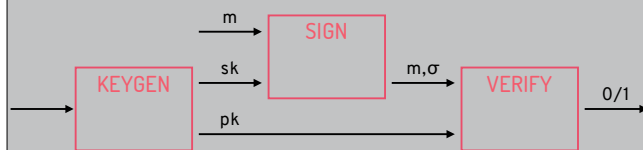
Correctness: Valid signatures using valid keys will verify properly (for all k,m and (pk,sk)∈[KeyGen(1^k)], Verify(pk,m,Sign(sk,m)) = 1)

Unforgeability (EUF-CMA): For a given public key, an adversary can't produce new signatures that verify ((pk,sk)←KeyGen(1^k), A gets pk and access to oracle Sign(m), can't output (σ,m) for m not queried to Sign)

4

Last week this was mainly in the form of digital signatures…

MACS
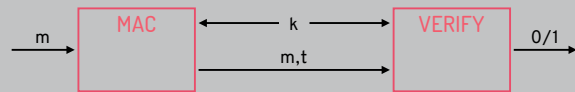
Correctness: Verify(k, m, MAC(k,m)) = 1

Unforgeability: hard to generate (m,MAC(k,m)) without knowing k

5

…MACs…

HASH FUNCTIONS

Two main security properties:
- **Pre-image resistance:** given $H(x)$ it's hard to find x
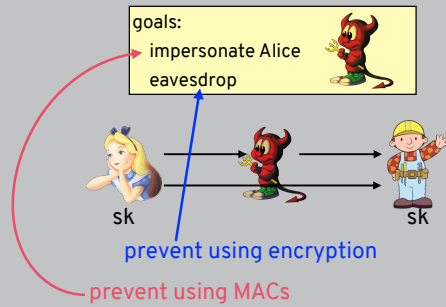- **Collision resistance:** it's hard to find x and y so that $x \neq y$ but $H(x) = H(y)$

Applications:
- File checksum
- MACs
- Digital signatures
- Commitments
- Blockchains
- Virus scanning (next week)
- Password storage (Week 7)
- …and many more!

6

…hash functions…

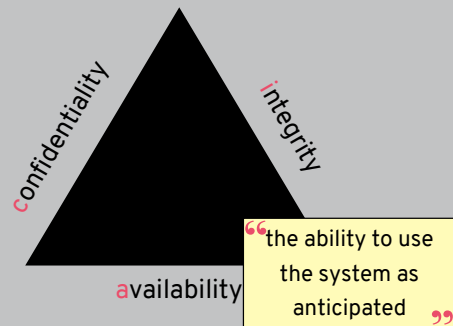…and probably the most advanced thing we saw was AEAD.

This week we'll complete the triangle by looking at availability