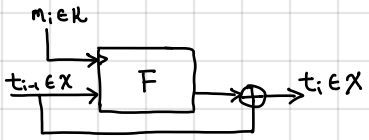
Sufficient now to construct a compression function.

Typical approach is to use a block cipher.

Davies-Meyer: Let $F: K \times X \to X$ be a block cipher. The Davies-Meyer compression function $h: K \times X \to X$ is then



$$h(k,x) := F(k,x) \oplus x$$

Many other variants also possible: $h(k,x) = F(k,x) \oplus k \oplus x$ [used in Whirlpool hash family]

Need to be careful with design!

- $h(k,x) = F(k,x)$ is not collision-resistant: $h(k,x) = h(k', F^{-1}(k', F(k,x)))$
- $h(k,x) = F(k,x) \oplus k$ is not collision-resistant: $h(k,x) = h(k', F^{-1}(k', F(k,x) \oplus k \oplus k'))$

Theorem. If we model F as an ideal block cipher (i.e., a truly random permutation for every choice of key), then Davies-Meyer is collision-resistant.

Conclusion: Block cipher + Davies-Meyer + Merkle-Damgård $\Rightarrow$ CRHFs

Examples: SHA-1: SHACAL-1 block cipher with Davies-Meyer + Merkle-Damgård ← no longer secure [first collision found in 2017!]

→ birthday attack run-time: $\sim 2^{80}$
attack ran in time $\sim 2^{64}$ (100,000× faster)

January, 2020: chosen-prefix collision in $\sim 2^{63.4}$ time!

- SHA-1 extensively used (e.g., git, svn, software updates, PGP/GPG signatures, certificates) → attacks show need to transition to SHA-2 or SHA-3

SHA-256: SHACAL-2 block cipher with Davies-Meyer + Merkle-Damgård

Why not use AES?

- Block size too small! AES outputs are 128-bits, not 256 bits (so birthday attack finds collision in 2^{64} time)
- Short keys means small number of message bits processed per iteration.
- Typically, block cipher designed to be fast when using same key to encrypt many messages
  - ↳ In Merkle-Damgård, different keys are used, so alternate design preferred (AES key schedule is expensive)

Recently: SHA-3 family of hash functions standardized (2015)

- ↳ Relies on different underlying structure ("sponge" function)
- ↳ Both SHA-2 and SHA-3 are believed to be secure (most systems use SHA-2 – typically much faster)

Back to building a secure MAC (or even better, a large-domain PRF) from a CRHF – can we do it more directly than using CRHF + small-domain MAC?

- ↳ Main difficulty seems to be that CRHFs are keyless but MACs are keyed

Idea: include the key as part of the hashed input

By itself, collision-resistance does not provide any "randomness" guarantees on the output

- ↳ For instance, if H is collision-resistant, then $H'(m) = m_0 \| \cdots \| m_{10} \| H(m)$ is also collision-resistant even though H' also leaks the first 10 bits/blocks of m
- ↳ Constructing a PRF/MAC from a hash function will require more than just collision resistance
  - Option 1: Model hash function as an "ideal hash function" that behaves like a fixed truly random function (modeling heuristic called the random oracle model – will encounter later in this course)
  - Option 2: Start with a concrete construction of a CRHF (e.g., Merkle-Damgård or the sponge construction) and reason about its properties
    - ↳ We will take this approach

Suppose H is a Merkle-Damgård hash function built from a secure compression function

Several ways to build a keyed function:

1. Prepend key: $F(k, m) := H(k \| m)$
   ↳ Insecure due to structure of Merkle-Damgård: can mount an "extension attack:" given $H(k \| m)$, can compute $H(k \| m \| m')$ by extending Merkle-Damgård chain
2. Append key: $F(k,m) := H(m \| k)$
   ↳ Similar to hash-then-MAC construction and vulnerable to same offline attack: adversary finds a collision in the Merkle-Damgård prefix and uses that to construct a forgery
   ↳ Structure exploited in SHA-1 collision demonstration (can generate arbitrary collisions once prefix matches) → for SHA-1, they used PDF files
3. Envelope method: $F(k,m) := H(k \| m \| k)$
4. Two-key nest: $F((k_1, k_2), m) := H(k_2 \| H(k_1 \| m))$

} for reasonable pseudorandomness assumptions on h (e.g., both $F_1(k,m) := h(k,m)$ and $F_2(k,m) := h(m,k)$ is a PRF), both of these constructions are secure PRFs on a variable-size domain

hash-based MAC

HMAC is a PRF/MAC based on the two-key nest (though with correlated keys):

$HMAC(k, m) := H(k_1 \| H(k_2, m))$

where $k_1 \leftarrow k \oplus ipad$ and $k_2 \leftarrow k \oplus opad$

and ipad and opad are fixed strings (specified in the HMAC standard)

0x36 repeated 0x5C repeated

Security: Since k_1 and k_2 are correlated, need to make stronger assumption on security (e.g., h remains pseudorandom under a related-key attack)

Instantiations: Typically, denoted HMAC-H where H is the hash function

e.g., HMAC-SHA1

HMAC-SHA256 — one of the most widely-used MAC on the web (used in SSL/TLS, IPsec, SSH, and more)

HMAC for key-derivation: Recall that under reasonable assumptions, HMAC is a secure PRF

In many protocols, we need to derive multiple keys from a single master key (e.g., derived from a password)

↳ To derive multiple independent cryptographic keys, a PRF is a natural primitive:

$k_{enc} \leftarrow HMAC(k_{master}, \text{"enc"})$

$k_{mac} \leftarrow HMAC(k_{master}, \text{"mac"})$

} PRF security says derived keys are computationally indistinguishable from uniform

derived keys master key tag (just has to be unique)

This approach is used in TLS and IPsec to derive session keys during session setup

↳ General paradigm is the "expand" step in hash-based key-derivation (HKDF — RFC 5869)

↳ Consists of two procedures:

- Extract: derive a master key from entropy source (e.g., a user password)
- Expand: derive sub-keys from the master key

Both steps rely on HMAC