\( a \rightarrow f(x[0]) \rightarrow f(x[1]) \rightarrow f(x[2]) \rightarrow f(x[3]) \rightarrow F(x) \)
\[ F(x) = f(x[0]) \cdot f(x[1]) \cdot f(x[2]) \cdot f(x[3]) \]
$f$ $f$ $f$ $f$

\[ \text{NMAC}_{k_1, k_2}(x) = F_{k_1}(F_{k_2}(x)) \]
\[ \text{NMAC}_{k_1,k_2}(x) = F_{k_1}(F_{k_2}(x)) \]
$$HMAC_k(x) = F(k \oplus opad \parallel F(k \oplus ipad \parallel x))$$
HMAC_k(x) = F(k ⊕ opad || F(k ⊕ ipad || x))
$\text{HMAC}_k(x) = F(k \oplus \text{opad} \ || \ F(k \oplus \text{ipad} \ || \ x))$
What Happens If the Hash Function Breaks?

- The security of the NMAC is related to the security of the underlying hash
- If someone can break NMAC, we can break the hash
- If someone comes up with an attack on a hash function, does that mean that NMAC with that hash is broken?
Short Answer: It Depends
Concrete Example

• Lots of systems use the hash function MD5 with HMAC - often notated HMAC-MD5

• Last month, it was shown that collisions can be found in MD5 (in about an hour)

• Thus, MD5 is not collision resistant

• Does that mean HMAC-MD5 isn’t a secure MAC?
If the keyed compression function $f$ is a (...)-secure MAC and the keyed iterated hash $F$ is (...)-weakly collision resistant, then NMAC is a (...)-secure MAC.
If the keyed compression function $f$ is a (...)-secure MAC and the keyed iterated hash $F$ is (...)-weakly collision resistant, then NMAC is a (...)-secure MAC.
If the keyed compression function $f$ is a (...)-secure MAC and the keyed iterated hash $F$ is (...)-weakly collision resistant, then NMAC is a (...)-secure MAC.
If the conditions of the theorem aren’t satisfied, it doesn’t mean NMAC is broken - just that we don’t have a proof that it’s secure.
Should we continue to use HMAC-MD5?