background report

What is a MAC and its purpose?

A **Message Authentication Code (MAC)** is a tool in cryptography that checks two things:

- The message has not been changed.
- The message came from the right person.

A MAC uses:

- A secret key shared between the sender and receiver
- The message to be checked

It creates a MAC tag, which is sent with the message. The receiver makes the MAC again using the same key and message. If both MACs match, the message is trusted.

MAC gives:

- **Integrity:** Finds any changes in the message
- **Authentication:** Only someone with the key can make the right MAC

Length Extension Attack (MD5 / SHA-1)

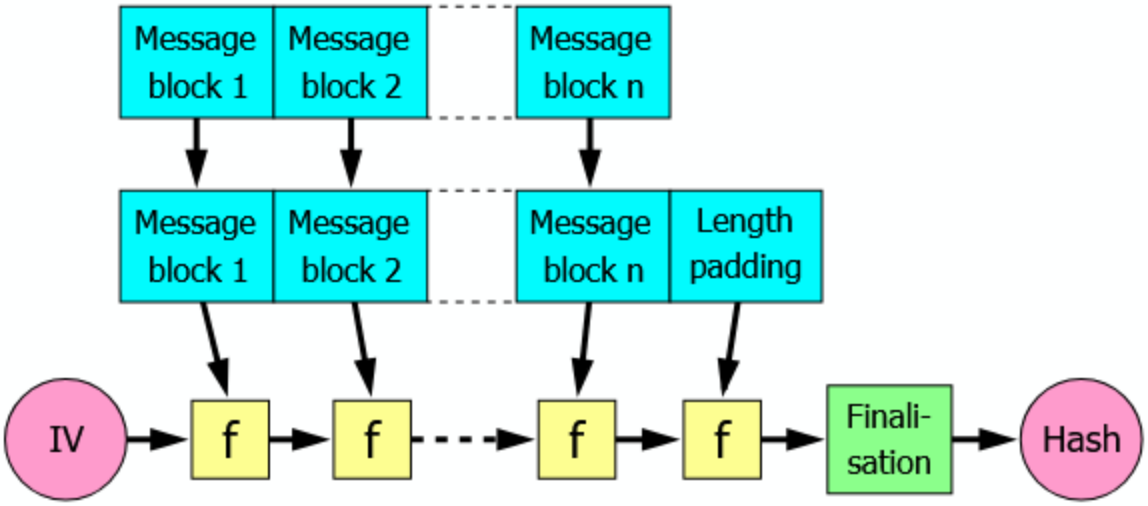
Some hash functions like **MD5** and **SHA-1** have a weakness called a **length extension attack**. This happens because they are made using something called the **Merkle–Damgård construction**.

What is Merkle–Damgård?

It is a way to build a hash function by:

- Breaking the message into small parts
- Processing one part at a time
- Saving the result after each step
- Giving the last result as the final hash

Because of this, hackers can add more data to the message and still get a valid hash, even without knowing the secret.



Conclusion

MACs ensure message integrity and authenticity, but naive MACs using MD5 or SHA-1 can be vulnerable to length extension attacks. This allows attackers to forge valid MACs by adding data without knowing the key. Secure methods like HMAC prevent this and keep communications safe.