A Suggestion for Handling Arbitrary-Length Messages with the CBC MAC

John Black and Phillip Rogaway

UNR UC Davis

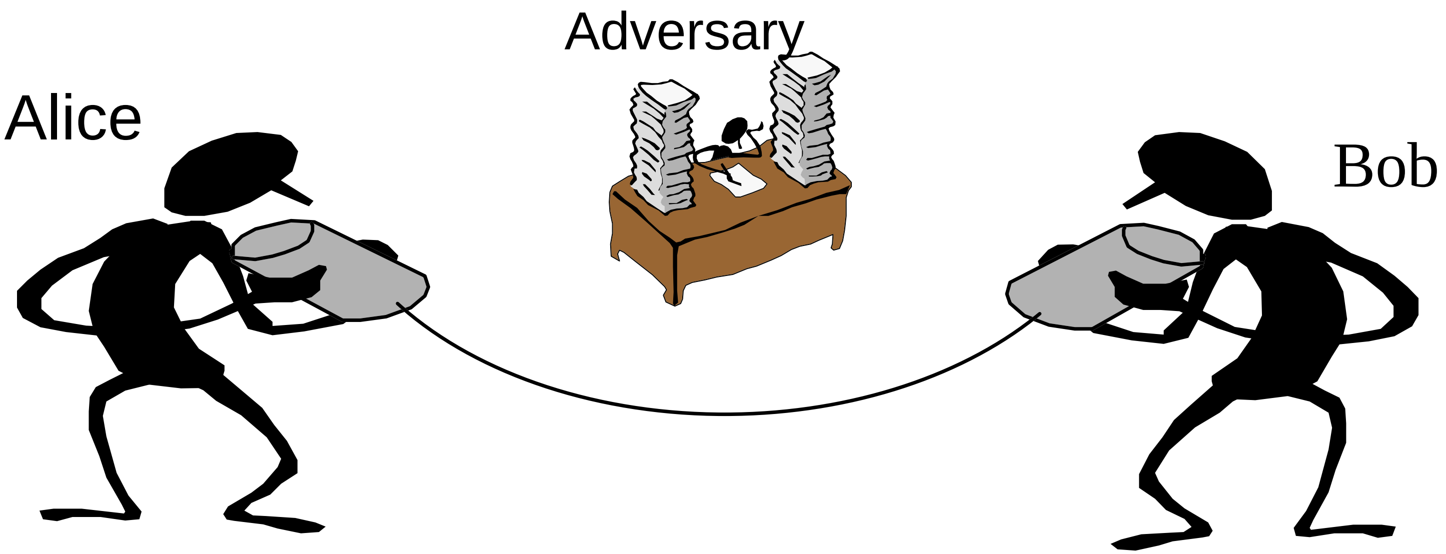
NIST Workshop

Baltimore, MD

October 20, 2000

What is a MAC?

Alice wishes to send Bob a message in such a way that Bob can be certain (with very high probability) that Alice was the true originator of the message.



What is the Goal?

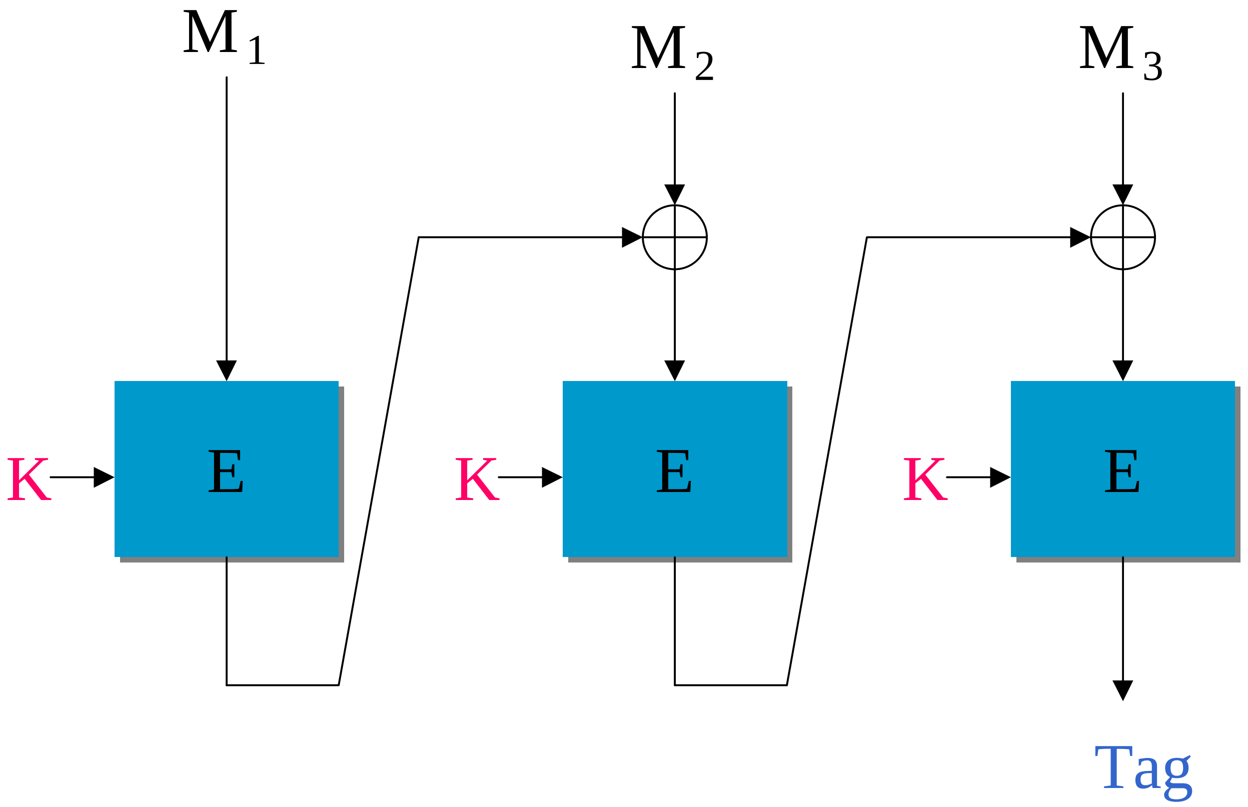
The adversary sees messages and their MACs, then attempts to produce a new message and valid MAC (aka a “forgery”).

Can easily produce valid MACs

Cannot produce valid MACs

The Basic CBC MAC

- ANSI X9.19, FIPS 113, ISO/IEC 9797-1
- Proven track record



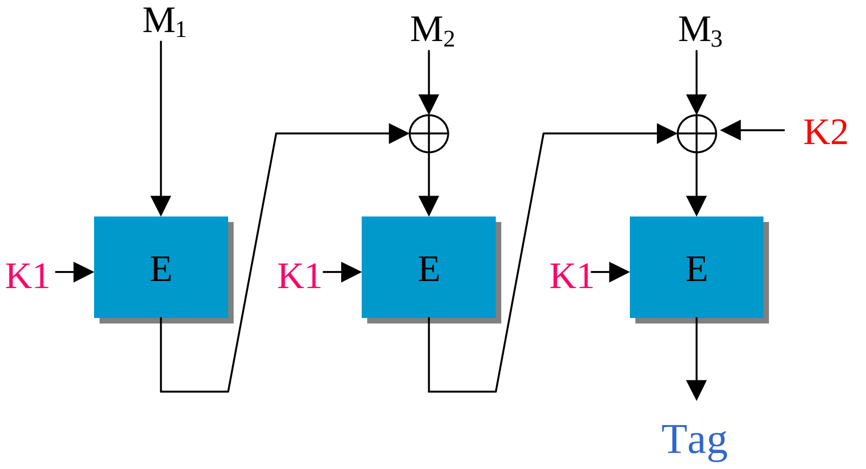
Length Variability

- Basic CBC MAC does not allow messages of varying lengths
- Several suggestions address this problem:
  - ANSI X9.19 (Optional Triple-DES)
  - Race Project (EMAC)
  - Knudsen, Preneel (MacDES)
  - Black, Rogaway (XCBC)

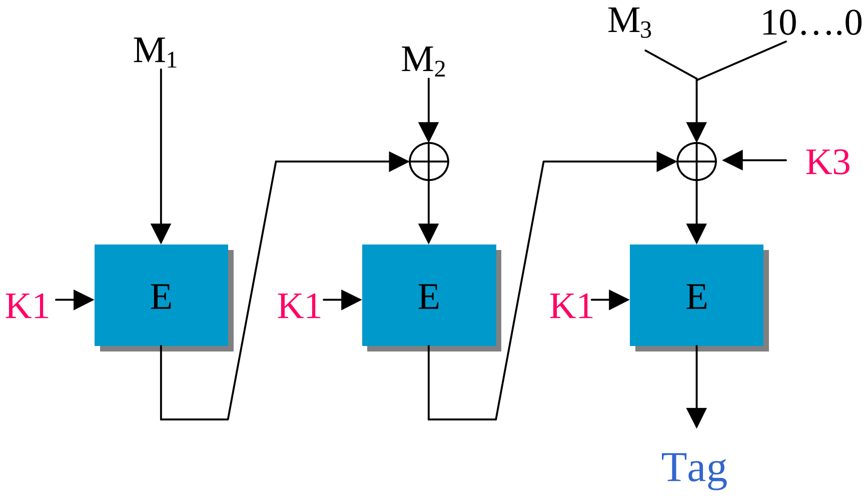
Accepting ALL Message Lengths

- Messages whose lengths are not a multiple of the block length are the norm
- Only the last suggestion allows messages of any length while remaining optimal
  - – Optimal is $\max\left\{1, \left\lceil |M|/128 \right\rceil\right\}$ for this style of MAC

Our Suggested Scheme



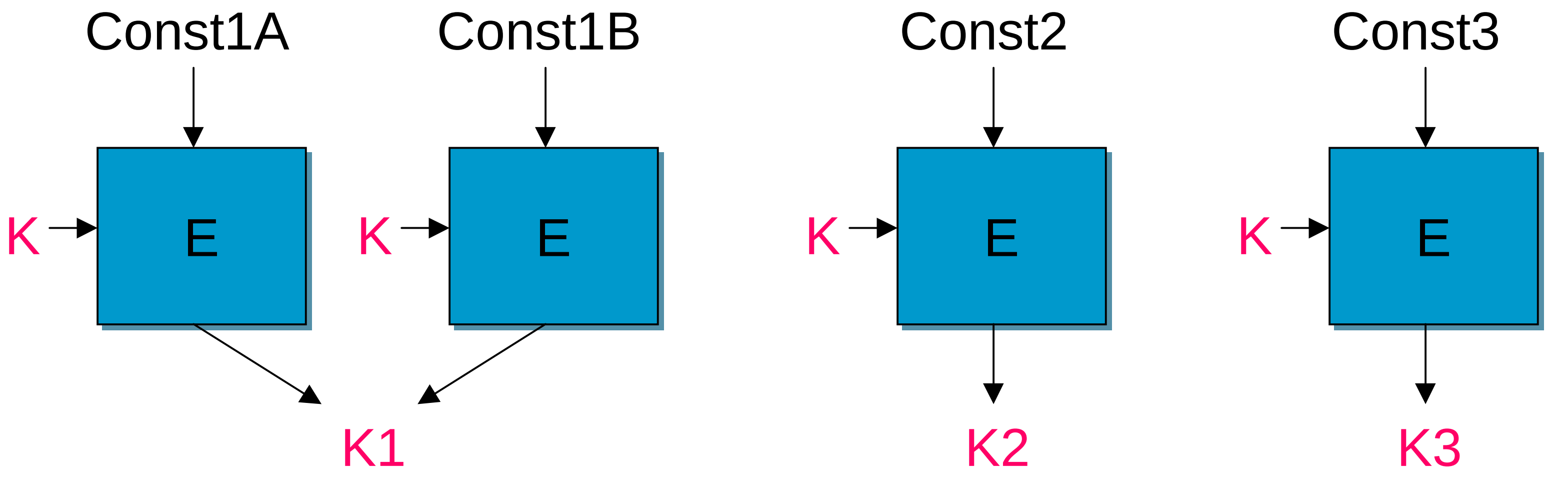
if |M| is a positive multiple of the block length (128 for AES)



otherwise

A Note on Deriving K1, K2, K3

- Under standard assumptions (ie, that E is a PRP) we can derive K1, K2, and K3 in the standard way:



Advantages

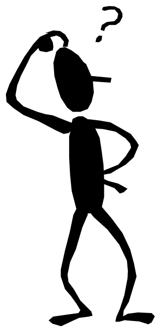
- Uses optimal number of block cipher invocations (for this style of MAC)
- Handles messages of any length
- Block cipher is invoked with only one key: K1
- Easy to implement, familiar to users
- Long history of resistance to attacks

Security

Thm: Assume E is a random block cipher. Then an adversary who makes at most q queries, each of at most mn bits ($m \leq 2^{n-2}$), can distinguish this CBC MAC construction from a random function with advantage at most

$$\mathrm{Adv}^{\mathrm{prf}}(m, q) = \frac{(4m^2 + 1)\, q^2}{2^n}$$

What Did That Mean?



- Concrete Example:
  - – Say our max message length is 10Kb
  - – An adversary watches 1,000 MAC tags go by every second for a month
  - – Adversary’s chance of forgery is less than one in a trillion

Drawbacks

- Hard to extract parallelism
  - Inherent in CBC MAC
- No added resistance to key-search attacks
  - Modern block ciphers with large keys (eg, AES) make this moot

Conclusion

- Suggested CBC MAC is ripe for standardization as a block cipher Mode of Operation
  - Simple
  - Efficient
  - Tested
  - Proven Security