Lecture 6 - 07/02/2017

The History of Message Authentication Codes

Clay Pots (8000 BC)

- A lot of ancient economies were debt based so during market excursions had to be secured by a signal that could not be tampered with

Cylinder Seal (3500 BC)

But, the above are physical authentication rather than informational authentication

WW2 era DRYAD authentication cipher

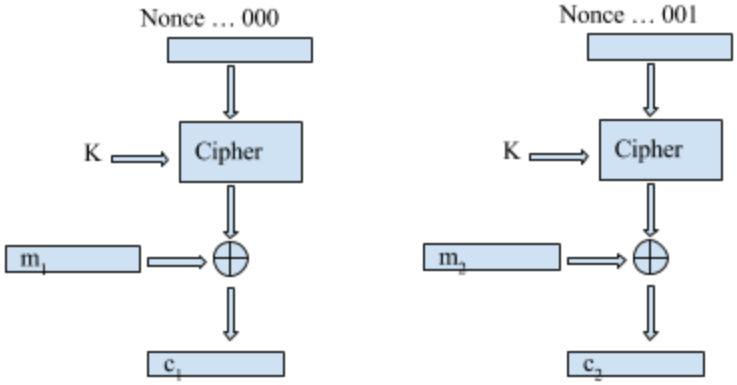
- The message itself is not secured, but the receiver is ascertained before the message can be read

Lecture

Alice sends a message to Bob

A_K $\rightarrow\rightarrow\rightarrow$ B_K

$c = CTR(k, m)$ c



If Eve, an active aggressor, changes one bit of the message → the decrypted message that Bob receives will be off by that one bit

While CTR may be great for Confidentiality, confidentiality is not the same as Authentication

A_K $\rightarrow\rightarrow\rightarrow$ B_K

t *is a tag* m, t $I = ver(k, t, m)$

$t = MAC(k, m)$

Is this secure?
MAC_K: $t \leftarrow MD5(k \| m)$

No, because of length extension
T' = MD5 (k || m || m')

What do we want from a MAC:

- Correctness
  - $Ver_K (m, Mac_K(m)) - 1$
- Security:

Ad	$\rightarrow \rightarrow \rightarrow$	$t = \{0,1\}^L$
	$m_1, m_2, \ldots, m_n$	L = 128 bits
	$\leftarrow \leftarrow \leftarrow$ *repeat*	
	$t_1, t_2, \ldots, t_n$	$Pr [Ver_K (m^*, t^*) = 1] \approx \frac{1}{2^L}$
	$\rightarrow \rightarrow \rightarrow$	
	m^*, t^*	

HMAC

Constraints opad and ipad where $opad \neq ipad$

$t = H [k \oplus opad \| H (K \oplus ipad \| m)]$

What are opad and ipad?

Number of the length of the key

There's a scheme where you can choose keys smaller than opad and ipad

Or the same key that when XORed with opad and ipad become different