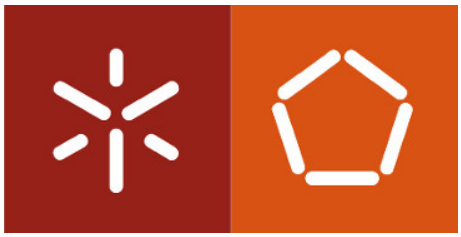
Tecnologia Criptográfica

13 de Dezembro de 2020

Trabalho Prático 4

a83899	André Morais
a84485	Tiago Magalhães

Falsificação CBCMAC



Mestrado Integrado em Engenharia Informática
Universidade do Minho

Conteúdo

1 Introdução

No âmbito da Unidade Curricular de Tecnologia Criptográfica, foi nos proposto para descrever como produziríamos uma falsificação considerando o CBCMAC, utilizando a cifra AES, para mensagens de tamanho fixo, igual a dois blocos do AES, para dois modos de enfraquecimento deste (utilização de vetor de inicialização aleatório e utilizando como *tag* todos os blocos do criptograma).

2 Estatégias de falsificação

Para um MAC(*message authentication code*) ser considerado seguro este tem de resistir a *chosen-plaintext attacks*, isto quer dizer, mesmo que um atacante tenha acesso a um oráculo, que possui a chave e gera *tags* para as mensagens do atacante, o atacante não pode adivinhar uma *tag* para novas mensagens (que não foram questionadas ao oráculo) sem realizar uma grande quantidade de computação. Também um MAC não deve possibilitar diferentes mensagens com a mesma *tag*.

2.1 Utilizando um IV aleatório

Considerando uma mensagem $M = (M_1||M_2)$, escolhendo um IV aleatório sabe-se que o último bloco do CBCMAC irá ser a *tag* e $A_1 = E(IV \oplus M_1)$ corresponderá ao primeiro bloco, deste modo sabemos que se conseguirmos arranjar M' tal que alteremos IV e M_1, mas mantenhamos o resultado de A_1 o último bloco ($A_2 = E(A_1 \oplus M_2)$) irá permanecer igual e por isso as *tags* serão iguais. Se construirmos $M' = (M'_1||M_2)$, para cada bit modificado em M'_1, como conhecemos IV, uma vez que é necessário que vá junto da *tag* para se poder verificar(IV's diferentes geram resultados diferentes), então podemos inverter o bit correspondente no IV originando deste modo IV'. O primeiro bloco desta mensagem M' corresponderá a $E(IV' \oplus M'_1)$, que será igual a A_1, devido aos bits de M'_1 e IV' terem sido invertidos nas mesmas posições, levando a que o resultado do $\oplus$ se mantenha, já que alterações em M'_1 irão ser "canceladas"por inversões em IV'.

Exemplo:

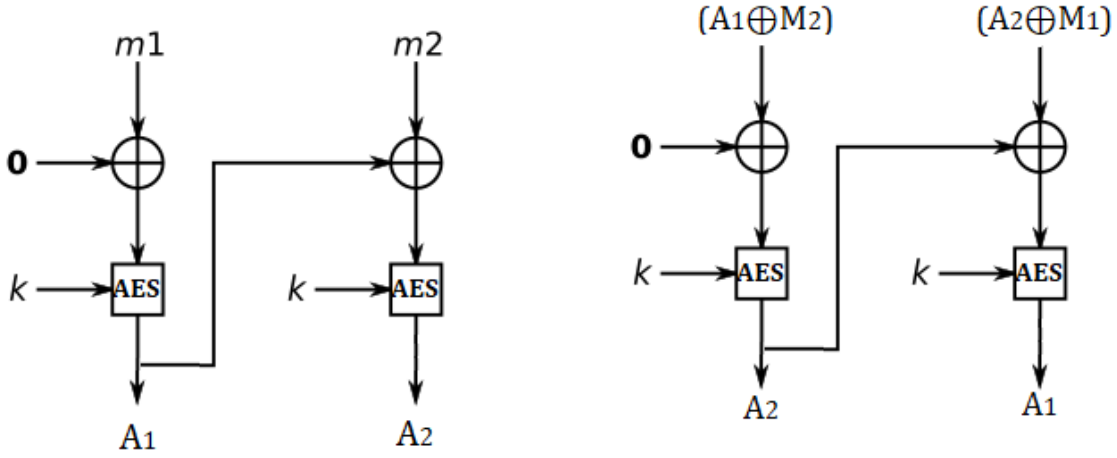
$M = (M_1||M_2)$, em que $M_1 = 001$, $M_2 = 010$ e $IV = 100$, com isto o resultado do primeiro bloco será $A_1 = E(IV \oplus M_1) = E(100 \oplus 001) = E(101)$, ao aplicarmos a técnica explicada acima construímos : $M' = (M'_1||M_2)$, em que $M'_1 = 101$ (inversão $1^{\underline{o}}$ bit em relação a M_1), $M_2 = 010$ e $IV = 000$ (como invertemos primeiro bit de M_1 aqui também o teremos de inverter), segue que o resultado do primeiro bloco será $E(IV' \oplus M'_1) = E(000 \oplus 101) = E(101)$, pela mensagem M sabemos que $E(101) = A_1$, como A_1 se mantém e M_2 também então o resultado do último bloco será igual e consequentemente a *tag*.

Desta forma conseguimos arranjar duas mensagens diferentes com a mesma *tag*, bem como arranjar uma tag para uma nova mensagem.

2.2 Utilizando como *tag* todos os blocos do criptograma

Neste método para enfraquecer este MAC, utilizamos como *tag* todos os blocos do criptograma, em vez de apenas o último bloco. Considerando também que os blocos de mensagem têm o mesmo tamanho (n) e o vetor de inicialização (IV) = 0^n, para não ser possível a falsificação explicada acima.

O atacante, interceta ou interroga o oráculo com a mensagem $M = (M_1||M_2)$ e obtém a *tag* $A = A_1||A_2$. Com isto sabe-se que: $A_1 = E(M_1)$ e $A_2 = E(A_1 \oplus M_2)$ (**Figura 1(a)**) e por isso, podemos construir $M' = (A_1 \oplus M_2)||(A_2 \oplus M_1)$, pela **Figura 1(b)** podemos ver que o resultado de $E(A_1 \oplus M_2) = A_2$, uma vez que $A_2 = E(A_1 \oplus M_2)$ pelo resultado do oráculo à mensagem M e A2 $\oplus$ $(A_2 \oplus M_1)$ irá dar M_1, ou seja, o segundo bloco da *tag* de M' terá como resultado $E(M_1) = A_1$, deste modo conseguimos produzir uma *tag* para uma mensagem nova sem interrogar o oráculo, sendo esta: $A' = (A_2||A_1)$, assim, verifica-se $Vrfy_k(M', A') = 1 \wedge (M', A') \notin Q$, isto é, o verificador vai então aceitar **M'** como válido, tal como a sua *tag* **A'**.



(a) Mensagem M

(b) Mensagem M'

Figura 1: CBC-MAC

3 Conclusão

Dado como terminado este trabalho, este permitiu-nos aprofundar os conhecimentos obtidos nas aulas teóricas, percebendo melhor na prática como a segurança de *message authentication code* pode ser comprometida.

Referências

[1] CBCMAC, disponível em:
`https://en.wikipedia.org/wiki/CBC-MAC`