Protocolos Criptográficos Avançados

Renan Menezes*

2019

Resumo

Conforme será apresentado nesse artigo, veremos como os Protocolos Criptográficos , tem avançado nesses últimos anos, pois com a crescente informatização dos serviços e a expansão do mundo tecnológicos, vem a preocupação com a segurança, o que leva muitas pessoas se questionar se estão realmente protegidas e como fazer para obter essa proteção nas redes.

O mercado de Criptografia vem aumentando fazendo com que cada dia, tengo grande parte de avanços que ajudam as pessoa mal intencionada a não conseguir de maneiras tão fáceis assim obter informações, que acabam sendo colocadas nas redes de formas corriqueiras.

Iremos abordar neste documento alguns protocolos de segurança, falando um pouco de como eles surgiram e como eles estão em bastante transformação.

Palavras-chaves: protocolos. Segurança.

Introdução

Na atualidade temos muitos padrões no lado da segurança, alguns que são muito utilizados, como o AES é a abreviação de Advanced Encryption Standard(Padrão Avançado de Criptografia). É uma codificação em bloco simétrica usada pelo governo americano para criptografar dados confidenciais. O AES também é usado por indivíduos e empresas para bloquear informações classificadas ou valiosas.

*renan.meneses@alu.ufc.br

Referências

ANEXO A – Historia da AES de 256 bits

A criptografia AES foi desenvolvida em respostas às necessidades governamentais, as agências confiaram no padrão a partir de 1977, ela se torna padrão, com seu algoritmo de chave simétrica de 56 bits, foi um sucesso por 20 anos, até que em 1990, insuficiente dado que na época poderia ser quebrado em 22 hora. Quando começou sua reformulação e novos desenvolvimento, a próxima foi a AES-64, depois veio AES-128 e foi evoluindo até o dia 26 de novembro de 2001, que foi lançada pela NIST a AES-256, que foi um , em 2002 foi adotada pelo EUA como padrão de criptografia adotada no país. Hoje, o AES é um sistema confiável, com ampla adoção. As bibliotecas AES foram desenvolvidas para linguagens de programação, incluindo C, C ++, Java, Javascript e Python. O AES é usado por programas de compactação de arquivos, incluindo 7 Zip, WinZip e RAR; sistemas de criptografia de disco como BitLocker e FileVault; e sistemas de arquivos como NTFS. É uma ferramenta importante na criptografia de banco de dados , bem como em sistemas VPN com IPsec e SSL / TLS. Os gerenciadores de senhas como LastPass, KeePass e 1Password usam o AES, assim como os programas de mensagens como o WhatsApp e o Facebook Messenger. Um conjunto de instruções AES é integrado a todos os processadores Intel e AMD. Até video games como Grand Theft Auto IV usam o AES para se proteger contra hackers.

ANEXO B – Vantagens e Desvantagens

Vantagens

Implementação:

- Roda bem e e rápido em relação a outros algorítimos.

- Pode ser implementado em um SmartCard usando pouca codigo e memoria.

- Podendo ser feitas em paralelos em algumas funções, dividindo o processamento e tornando mais rapido.

- Como não utilizar operações aritméticas, não exige muito poder de processamento.

Possibilidade de modificações:

- Permite a alteração da chave em 32 e 32 bits, sendo iniciado em 128 bits ate 256 bits.

- Pode fazer a alteração de paramentos, mas não de rodadas.

Simplicidade de Projeto:

- Não usa elementos previamente processados.

- O algoritmo não baseia sua segurança ou parte dela em interações obscuras e não bem compreendidas entre operações aritméticas, não permitindo assim, espaço para esconder um trap-door.

Desvantagens

- A inversa é menos recomendável de ser implementada num SmartCard, pois precisa de mais código e mais processamento. Mesmo assim, se comparado, a outros algoritmos ela bem rápida.

- Em hardware só pode usar um parte do circuito usando no processo de encriptação.

- Em código a encriptação e sua inversão só pode ser usado em códigos diferentes.

ANEXO C – Funcionamento da AES-256

O método mais comum de atacar uma cifra de bloco é tentar vários ataques em versões dele com um número menor de rodadas. O AES tem 10 rodadas para chaves de 128 bits, 12 rodadas para chaves de 192 bits e 14 rodadas para chaves de 256 bits. Até 2005, os ataques mais conhecidos estão em versões reduzidas para 7 rodadas para chaves de 128 bits, 8 rodadas para chaves de 192 bits e 9 rodadas para chaves de 256 bits. Este fato, no entanto, traz preocupação a alguns criptógrafos, pois consideram que a margem entre o número de rodadas especificado na cifra e os ataques mais conhecidos é muito pequena, o que corre o risco de encontrar alguma forma de melhorar os ataques. Para Arian, a segurança de seu sistema de computador é de vital importância, por isso a proteção dos dados de nossos usuários e a segurança de nossos processos é uma de nossas principais características. É aqui que entra a criptografia, um procedimento para modificar as informações, tornando-as incompreensíveis para todos aqueles que não possuem uma chave secreta. Todas as operações no AES tratam os bytes de entrada como um corpo finito (finite fields, ou Galois fields) em 28. Isso significa que: Há um conjunto [0,255] (que são todos os valores possíveis para um byte) e um desses elementos é chamado "zero"(no caso, o próprio 0); Há uma operação, que chamaremos de "adição", que se aplica a quaisquer dois elementos nesse conjunto e cujo resultado também é um elemento desse conjunto. Essa operação precisa ser associativa, comutativa, possuir elemento neutro, e cada elemento deve ter um inverso; Nesse caso, definimos a "adição"como o "OU exclusivo- XOR. Há uma operação, que chamaremos de "multiplicação", com características semelhantes à "adição". Exceto pelo elemento "zero", que não tem inverso (e o elemento neutro da multiplicação é chamado de "um"). A multiplicação também precisa ser distributiva em relação à adição.

A "multiplicação"será definida adiante. Para quem não tem experiência com matemática, é bom frisar que estamos definindo "adição", "multiplicação", "zero"e "um- esses nomes não têm necessariamente nada a ver com as operações aritméticas usuais que fazemos no conjunto dos números Naturais ou Reais (os Naturais ou Inteiros, por exemplo, não formam corpos com o + e * usuais, pois não existe x dentro desses conjuntos tal que 2*x=1; os Reais formam um corpo, só que infinito). Não há "subtração", "divisão", etc.

A adição, como já foi dito, foi definida como sendo o XOR. A multiplicação é mais complexa: primeiro trate cada operando como se fosse um polinômio com base na sua representação binária (ex.:

$\boxed{\text{6 - 110 - vira } x^2 + x, e 11 - 1011 - vira x^3 + x + 1)}$

, multiplique-os, depois divida o resultado por um "agente redutor".
O resto da divisão (interpretado novamente como um número) será então o resultado da multiplicação.
No caso do AES, o agente redutorescolhido foi:

$$\boxed{x^8 + x^4 + x^3 + x + 1}$$

De modo que multiplicar 6 por 11 é o mesmo que fazer

$\boxed{(x^2 + x) * (x^3 + x + 1) mod(x^8 + x^4 + x^3 + x + 1)}$

$\boxed{=[(x^5 + x^3 + x^2) + (x^4 + x^2 + x)] mod(x^8 + x^4 + x^3 + x + 1)}$

$\boxed{=(x^5 + x^4 + x^3 + x) mod(x^8 + x^4 + x^3 + x + 1)}$

$\boxed{=111010 \text{ mod } 100011011}$

$\boxed{=111010}$

$\boxed{=58}$

Note que os coeficientes são "somados"usando o XOR, não a soma comum: quando se somou x^2 $com x^2 o resultado é zero, então 2 * x^2$.

Pensenessasomacomo

$\boxed{\mathbf{1*}x^2 + 1 * x^2 = (1 xor 1) * x^2 = 0 * x^2 = 0.}$

OcorpoGF($\mathbf{2^8}$)

$foiconstruídocombasenoboxed{\mathbf{GF(2)}}(corpobinário, ondeasomaéXOReamultiplicaçãoéAND), demodoqueseusp$

$Ouseja, umaimplementação[nãootimizada]doAESpoderiaporexemplocriarumtipode$

$dadodistintopararepresentarcadabytedasentradas/saídas/chavesedarsuaprópriaimplementaçãoda"adição$

$Issosimplificariaalógica, àscustasdaperformance.$