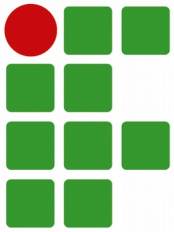


INSTITUTO FEDERAL
Goiás

Bacharelado em Sistema de Informação

Disciplina

Criptografia

2016

Aluno: João Manoel

INSTITUTO FEDERAL
Goiás

Criptografia - Introdução

- **Definição:** é o estudo da transformação do texto claro ou aberto em texto não legível (cifrado). A palavra Criptografia é derivada das palavras gregas “Kryptos” que significa “secreto” e “Graphein” que significa “escrita”. É comum que a criptografia seja confundida com criptoanálise (a tentativa de descobrir um texto cifrado) e criptologia (estudos matemáticos, computacionais, psicológicos entre outros, necessários à criptoanálise e criptografia).

- **Histórico:** Apesar de ser uma ferramenta amplamente utilizada no mundo contemporâneo, a criptografia possui origem milenar, tendo sido utilizada inclusive no Antigo Egito, cerca de 1900 A.C. onde há relatos de sua primeira aplicação de forma documentada. Os egípcios aplicavam a criptografia desenhando hieróglifos fora dos padrões.

Criptografia - Enigma

- **2ª Guerra Mundial:** A máquina Enigma era usada pelos alemães para criptografia. Os alemães acreditavam que o código da Enigma era inquebrantável.

- **Enigma@Home:** é um projeto BOINC que cria uma interface entre a rede BOINC e o Projeto M4. Responsável por decodificar duas das três últimas mensagens conhecidas que haviam sido criptografadas pela Enigma.

- **M4 Message Breaking Project:** Em 14/01/2013 foi decodificada, por Dan Girard, a última mensagem conhecida que havia sido criptografada pela Enigma, esse processo levou cerca de dez anos.

INSTITUTO FEDERAL
Goiás

Criptografia - Enigma

- **Texto Cifrado:**

HCEYZTCSOPUPPZDICQRDLWXXFACTTJMBRDVCJJMMZRPYIKHZAWGLYX
WTMJPQUEFSZBOTVRLALZXWVXTSLFFFAUDQFBWRRYAPSBOWJMKLDUY
UPFUQDOWVHAHCDWAUARSWTKOFVOYFPUFHVZFDGGPOOVGRMBPXX
ZCANKMONFHXPCKHJZBUMXJWXKAUODXZUCVCXPFT

- **Texto Simples:**

BOOTKLARXBEIJSCHNOORBETWAZWOSIBENXNOVXSECHSNULCBMXPR
OVIANTBISZWONULXDEZXBENOETIGEGLMESERYNOCHVIEFKLHRXSTEH
EMARQUBRUNOBRUNFZWOFUHFXLAGWWIEJKCHAEFERJXNNTWWWFU
NFYEINSFUNFMBSTEIGENDYGUTESIWXDVVVJRASCH

Criptografia - Enigma

- **Texto simples com as divisões de palavras, e com letras ilegíveis corrigido:**

  BOOT KLAR X BEI J SCHNOOR J ETWA ZWO SIBEN X NOV X SECHS NUL CBM X PROVIANT BIS ZWO NUL X DEZ X BENOETIGE GLAESER Y NOCH VIER KLAR X STEHE MARQU BRUNO BRUNO ZWO FUNF X LAGE WIE J SCHAEFER J X NNN WWW FUNF Y EINS FUNF MB STEIGEND Y GUTE SICHT VVV J RASCH

- **Texto simples formatado para o alemão:**

  Boot klar. Bei “Schnoor” etwa 27. Nov. 60 cbm. Proviant bis 20 Dez. Benötige Gläser, noch 4 klar. Stehe Marqu. BB 25. Lage wie “Schaefer”. NW 5, 15 mb steigend, gute Sicht. Von “Rasch”.

Criptografia - Enigma

- **Texto simples em português com adaptações entre colchetes:**

  Barco clara. [Será encontro] em Schnoor cerca de 27 de novembro. 60 metros cúbicos [óleo combustível restantes], disposições [suficientes] até 20 de Dezembro. Precisa de binóculos; [Somente] quatro agora utilizável. Estou na praça naval BB 25. Situação como Schaefer de. [Vento] noroeste [força] 5, [pressão atmosférica] 15 milibares subindo, boa visibilidade. De Rasch.

INSTITUTO FEDERAL
Goiás

Criptografia – Chave Simétrica

Figura 1. Chave simétrica

Criptografia – Chave Simétrica

Uma chave simétrica de 3 bits, pode ser um dentre os seguintes valores:

000
001
010
011
100
101
110
111

Isto nos dá apenas 8 possibilidades para k. Na matemática, o número de possíveis chaves é de 2 elevando ao número de bits (2^3 = 8).

Assim sendo, se um algoritmo simétrico tiver 128 bits de chave, como é o caso do AES, significa que ele tem 2^128 possíveis chaves ou 340282366920938463463374607431768211456.

Com um computador de 1 bilhão de cálculos por segundo e dispondo de 1 bilhão destes para usar, levaria 170141183460469231731 segundos, já considerando a metade das tentativas (2^127 - ninguém é tão azarado de acertar na última), em anos, chega-se a estrondosa quantia de 5.395.141.535.403 anos!

Literaturas afirmam que um algoritmos simétrico de 256 bits tem segurança eterna, pois nem todo o silício do universo daria para construir uma máquina que o quebrasse. Alguns cientistas vem falando da computação quântica e de como ela mudaria a maneira de fazer as coisas. Computação quântica é cercada de mistério e de exageros. O fato é que já existe uma máquina com sete bits quânticos disponível.

Criptografia – AES

- **Definição:** Advanced Encryption Standard (AES, ou Padrão de Criptografia Avançada, em português), também conhecido por Rijndael, é o padrão de criptografia adotado pelo governo dos Estados Unidos.

- **Histórico:** O AES foi anunciado pelo NIST (National Institute of Standards and Technology, ou Instituto Nacional de Padrões e Tecnologia em português) como U.S. FIPS PUB (FIPS 197) em 26 de Novembro de 2001, depois de 5 anos de um processo de padronização. Tornou-se um padrão efetivo em 26 de Maio de 2002. Em 2006, o AES já é um dos algoritmos mais populares usados para criptografia de chave simétrica.

Criptografia – AES

Numa proposta de substituir o DES (Data Encryption Standard), o NIST promoveu uma competição para que fosse feito um algoritmo que seria chamado AES (Advanced Encryption Standard) que atendesse as seguintes especificações:

- Algoritmo publicamente definido
- Ser uma cifra simétrica de bloco
- Projetado para que o tamanho da chave possa aumentar
- Implementável tanto em hardware quanto em software
- Disponibilizado livremente ou em acordo com termos ANSI

Criptografia – AES

Onde o AES foi julgado:

- Segurança (esforço requerido para criptoanálise)
- Eficiência computacional
- Requisitos de memória
- Adequação a hardware e software
- Simplicidade

O processo seletivo teve inicio em 1997 e terminou em 2000 com a vitória do algoritmo Rijndael escrito por Vincent Rijmen e Joan Daemen.

Este algoritmo criptografa e descriptografa usando uma chave criptografada e blocos, ambos de tamanhos de 128, 192 ou 256 bits.

Criptografia – AES

- **Vantagens quanto à implementação:**
  - Pode rodar bem rapidamente em relação a outros algoritmos.
  - Pode ser implementado em um SmartCard usando pouco código e memória.
  - Algumas funções podem ser feitas em paralelo, assim tornando o processo mais rápido.
  - Como a encriptação não emprega operações aritméticas, não exige muito poder de processamento.

Criptografia – AES

- **Vantagens quanto à simplicidade do projeto:**
  - Não usa elementos já previamente processados, por ex. a 9a rodada não necessita de nenhum elemento das rodadas anteriores a não ser única e exclusivamente do *estado* da 8a.
  - 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.

Criptografia – AES

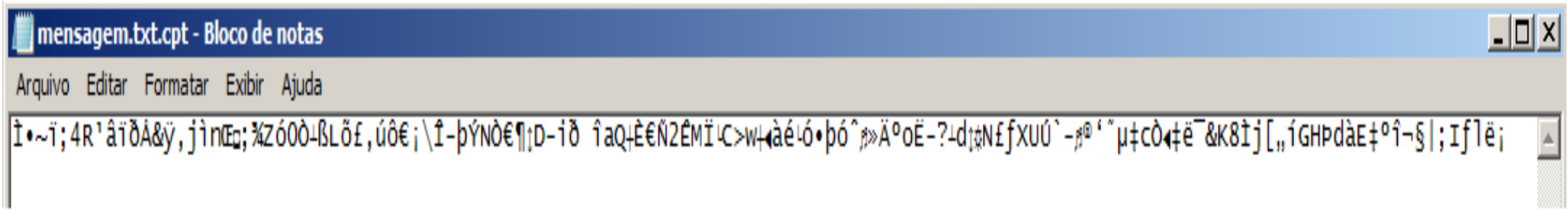
- **Vantagens quanto à possíveis modificações:**
  - O projeto permite a especificação de variantes com o comprimento do bloco e da chave, ambos variando de 32 em 32 bits no intervalo de 128 até 256 bits.
  - Embora o número das rodadas seja fixo na especificação, pode ser modificado como um parâmetro caso haja problemas de segurança.

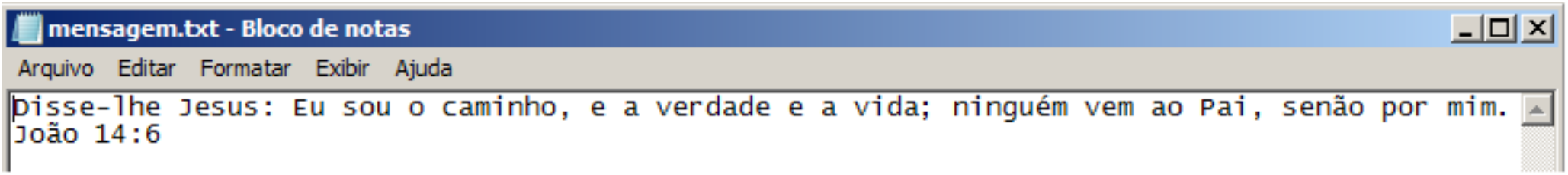
Criptografia – AES

- **As Desvantagens ficam por conta da inversa:**
  - 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 software, a encriptação e sua inversa empregam códigos diferentes e/ou tabelas.
  - Em hardware a inversa pode usar apenas uma parte do circuito usado no processo de encriptação.

Criptografia – AES

Mensagem criptografada utilizando o comando “ccrypt”:





INSTITUTO FEDERAL
Goiás

Criptografia – Chave Assimétrica

Figura 2. Chave assimétrica

Agora o que muitos realmente confundem é quanto a força bruta dos algoritmos assimétricos! É muito, mas muito diferente!

Em um simétrico, se eu tenho 8 bits de chave, tenho 256 combinações possíveis.

Se pegar o caso do RSA que é um assimétrico e se tiver uma chave de 8 bits, significa que o valor do N é de 256 bits. Sem querer descrever o RSA aqui, podemos dizer que N é o resultado da multiplicação de dois números primos de 4 bits. Quebrar a chave significa achar um destes números. E não é de 2^4 tentativas, pois os valores 2, 4, 6, 8, 9, 10 não precisam ser testados pois não são primos!

No universo de 4 bits só existem estes primos: 2, 3, 5, 7, 11 e 13. Só isso! Mata-se em seis tentativas no máximo!

Para algoritmos assimétricos, como no caso do RSA, o cálculo do esforço matemático não é simplesmente de 2^B (B = Número de bits). É muito, mas muito menos que isto.

Exatamente por isto é que os algoritmos assimétricos precisam de uma chave muito maior, hoje perto dos 1024 bits. No caso do RSA, dizer que ele é de 1024 bits, significa que o valor de N é de 1024 bits, logo, quebrar significa encontrar um número primo de até 512 bits que sirva.

Aí tem gente que se acostumou a ver o RSA de 1024 bits e sai dizendo que um AES de 128 é fraco, pois são só 128 bits! Porém, são coisas muito diferentes!

Criptografia – PGP

- **Definição do PGP:** PGP, do inglês Pretty Good Privacy (Privacidade Muito Boa), é um programa de computador de encriptação e descriptografia de dados (criptografia de chave assimétrica) que fornece autenticação e privacidade criptográfica para comunicação de dados.

- **Histórico do PGP:** O PGP foi criado no início da década de 90 e muitas vezes é confundido como um algoritmo de criptografia, um conceito equivocado. O PGP é um software inicialmente desenvolvido por Phil Zimmermann nos Estados Unidos, que adaptou conceitos já existentes da criptografia, no intuito de criar um sistema de fácil utilização,possibilitando até mesmo para uma pessoa comum a utilização da criptografia em seu dia a dia, desde que tivesse em mãos um computador.

Criptografia – PGP

- **Definição do PGP:** PGP, do inglês Pretty Good Privacy (Privacidade Muito Boa), é um programa de computador de encriptação e descriptografia de dados (criptografia de chave assimétrica) que fornece autenticação e privacidade criptográfica para comunicação de dados.

- **Histórico do PGP:** O PGP foi criado no início da década de 90 e muitas vezes é confundido como um algoritmo de criptografia, um conceito equivocado. O PGP é um software inicialmente desenvolvido por Phil Zimmermann nos Estados Unidos, que adaptou conceitos já existentes da criptografia, no intuito de criar um sistema de fácil utilização,possibilitando até mesmo para uma pessoa comum a utilização da criptografia em seu dia a dia, desde que tivesse em mãos um computador.

INSTITUTO FEDERAL
Goiás

Criptografia – PGP

- Problema com o governo dos EUA
- Zimmermann publicou um livro com o código fonte do PGP
- Zimmermann respondeu a vários processos e acabou inocentado
- PGP acabou se transformando em um software fechado
- Em 1998, a PGP Corporation lança o OpenPGP
- Os dois softwares (PGP e OpenPGP) se diferenciam pelo suporte, algoritmos de criptografia e transparência
- Em 1999, a Free Software Foundation desenvolveu o GNU Privacy Guard (GPG), o padrão atualmente para PGP, possui diversas interfaces gráficas (Seahorse, Kleopatra, Mailvelope, Enigmail, GPA, etc).

Criptografia – PGP

Os três pilares do PGP:

- **Confidencialidade:** Visa garantir que ninguém que não possua as chaves criptográficas possa visualizar o conteúdo de uma determinada mensagem. Esse pilar define o segredo que a mensagem cifrada se torna ao esconder o texto simples. Não é difícil que uma mensagem seja interceptada durante a sua transmissão, o PGP deve impedir que o conteúdo da mesma seja inteligível para quem não deve.
- **Integridade:** Este pilar estabelece de que uma mensagem não sofrerá alterações durante a sua transmissão, a forma que ela foi enviada será exatamente a forma que ela será recebida. O sistema OpenPGP possui um mecanismo de notificação que avisa o destinatário caso a mensagem tenha sofrido alguma alteração após o seu envio.

Criptografia – PGP

- **Não repúdio:** Este fundamento procura evitar que uma mensagem recebida com a assinatura digital do remetente não possa ser negada por ele, em outras palavras, a partir do momento em que se assina digitalmente uma mensagem com uma chave privada, está sendo comprovado de que o remetente da mensagem é a mesma pessoa que a escreveu, e ela não pode repudiar este fato. É recomendável que as mensagens cifradas sempre sejam assinadas digitalmente para prevenir possíveis tentativas de envio de mensagens falsas.
- **Autenticidade:** A união dos três pilares descritos acima, se aplicada de forma correta numa transmissão de mensagem, garante a autenticidade da mesma, ou seja, o destinatário pode ter certeza de que foi alguém conhecido que lhe enviou a mensagem, através da assinatura, pode comprovar que a mensagem não foi vista em sua transmissão ou adulterada.

Criptografia – PGP

O PGP é muito utilizado em mensagens enviadas via e-mail, tanto que boa parte de seus softwares derivados possuem plugins para se adaptarem aos gerenciadores de e-mail de seus usuários.

É o caso do Mailvelope - https://www.mailvelope.com/ - que usaremos numa demonstração a seguir.

INSTITUTO FEDERAL
Goiás

Criptografia – Bibliografia

- https://www.vivaolinux.com.br/artigo/Introducao-a-criptografia?pagina=6
- https://pt.wikipedia.org/wiki/Advanced_Encryption_Standard
- http://dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/edilson_fernandes.pdf
- http://rabci.org/rabci/sites/default/files/Artigo_Criptografia.pdf
- https://pt.wikipedia.org/wiki/OpenPGP


INSTITUTO FEDERAL
Goiás
Bacharelado em Sistema de Informação
Disciplina
Criptografia
2016
Aluno:
João Manoel

INSTITUTO FEDERAL
Goiás

Criptografia - Introdução

- **Definição:** é o estudo da transformação do texto claro ou aberto em texto não legível (cifrado). A palavra Criptografia é derivada das palavras gregas “Kryptos” que significa “secreto” e “Graphein” que significa “escrita”. É comum que a criptografia seja confundida com criptoanálise (a tentativa de descobrir um texto cifrado) e criptologia (estudos matemáticos, computacionais, psicológicos entre outros, necessários à criptoanálise e criptografia).

- **Histórico:** Apesar de ser uma ferramenta amplamente utilizada no mundo contemporâneo, a criptografia possui origem milenar, tendo sido utilizada inclusive no Antigo Egito, cerca de 1900 A.C. onde há relatos de sua primeira aplicação de forma documentada. Os egípcios aplicavam a criptografia desenhando hieróglifos fora dos padrões.

INSTITUTO FEDERAL
Goiás

Criptografia - Enigma

- **2ª Guerra Mundial:** A máquina Enigma era usada pelos alemães para criptografia. Os alemães acreditavam que o código da Enigma era inquebrantável.

- **Enigma@Home:** é um projeto BOINC que cria uma interface entre a rede BOINC e o Projeto M4. Responsável por decodificar duas das três últimas mensagens conhecidas que haviam sido criptografadas pela Enigma.

- **M4 Message Breaking Project:** Em 14/01/2013 foi decodificada, por Dan Girard, a última mensagem conhecida que havia sido criptografada pela Enigma, esse processo levou cerca de dez anos.

INSTITUTO FEDERAL
Goiás

Criptografia - Enigma

- **Texto Cifrado:**

HCEYZTCSOPUPPZDICQRDLWXXFACTTJMBRDVCJJMMZRPYIKHZAWGLYX
WTMJPQUEFSZBOTVRLALZXWVXTSLFFFAUDQFBWRRYAPSBOWJMKLDUY
UPFUQDOWVHAHCDWAUARSWTKOFVOYFPUFHVZFDGGPOOVGRMBPXX
ZCANKMONFHXPCKHJZBUMXJWXKAUODXZUCVCXPFT

- **Texto Simples:**

BOOTKLARXBEIJSCHNOORBETWAZWOSIBENXNOVXSECHSNULCBMXPR
OVIANTBISZWONULXDEZXBENOETIGEGLMESERYNOCHVIEFKLHRXSTEH
EMARQUBRUNOBRUNFZWOFUHFXLAGWWIEJKCHAEFERJXNNTWWWFU
NFYEINSFUNFMBSTEIGENDYGUTESIWXDVVVJRASCH

INSTITUTO FEDERAL
Goiás

Criptografia - Enigma

- **Texto simples com as divisões de palavras, e com letras ilegíveis corrigido:**

  BOOT KLAR X BEI J SCHNOOR J ETWA ZWO SIBEN X NOV X SECHS NUL CBM X PROVIANT BIS ZWO NUL X DEZ X BENOETIGE GLAESER Y NOCH VIER KLAR X STEHE MARQU BRUNO BRUNO ZWO FUNF X LAGE WIE J SCHAEFER J X NNN WWW FUNF Y EINS FUNF MB STEIGEND Y GUTE SICHT VVV J RASCH

- **Texto simples formatado para o alemão:**

  Boot klar. Bei “Schnoor” etwa 27. Nov. 60 cbm. Proviant bis 20 Dez. Benötige Gläser, noch 4 klar. Stehe Marqu. BB 25. Lage wie “Schaefer”. NW 5, 15 mb steigend, gute Sicht. Von “Rasch”.

INSTITUTO FEDERAL
Goiás

Criptografia - Enigma

- **Texto simples em português com adaptações entre colchetes:**

  Barco clara. [Será encontro] em Schnoor cerca de 27 de novembro. 60 metros cúbicos [óleo combustível restantes], disposições [suficientes] até 20 de Dezembro. Precisa de binóculos; [Somente] quatro agora utilizável. Estou na praça naval BB 25. Situação como Schaefer de. [Vento] noroeste [força] 5, [pressão atmosférica] 15 milibares subindo, boa visibilidade. De Rasch.

INSTITUTO FEDERAL
Goiás

Criptografia – Chave Simétrica

Figura 1. Chave simétrica

Auditoria e Segurança de Sistemas de Informação

Bacharelado em Sistema de Informação – 7º Período

2016

Criptografia – Chave Simétrica

Uma chave simétrica de 3 bits, pode ser um dentre os seguintes valores:

000
001
010
011
100
101
110
111

Isto nos dá apenas 8 possibilidades para k. Na matemática, o número de possíveis chaves é de 2 elevando ao número de bits (2^3 = 8).

Assim sendo, se um algoritmo simétrico tiver 128 bits de chave, como é o caso do AES, significa que ele tem 2^128 possíveis chaves ou 340282366920938463463374607431768211456.

Com um computador de 1 bilhão de cálculos por segundo e dispondo de 1 bilhão destes para usar, levaria 170141183460469231731 segundos, já considerando a metade das tentativas (2^127 - ninguém é tão azarado de acertar na última), em anos, chega-se a estrondosa quantia de 5.395.141.535.403 anos!

Literaturas afirmam que um algoritmos simétrico de 256 bits tem segurança eterna, pois nem todo o silício do universo daria para construir uma máquina que o quebrasse. Alguns cientistas vem falando da computação quântica e de como ela mudaria a maneira de fazer as coisas. Computação quântica é cercada de mistério e de exageros. O fato é que já existe uma máquina com sete bits quânticos disponível.

INSTITUTO FEDERAL
Goiás

Criptografia – AES

- **Definição:** Advanced Encryption Standard (AES, ou Padrão de Criptografia Avançada, em português), também conhecido por Rijndael, é o padrão de criptografia adotado pelo governo dos Estados Unidos.

- **Histórico:** O AES foi anunciado pelo NIST (National Institute of Standards and Technology, ou Instituto Nacional de Padrões e Tecnologia em português) como U.S. FIPS PUB (FIPS 197) em 26 de Novembro de 2001, depois de 5 anos de um processo de padronização. Tornou-se um padrão efetivo em 26 de Maio de 2002. Em 2006, o AES já é um dos algoritmos mais populares usados para criptografia de chave simétrica.

INSTITUTO FEDERAL
Goiás

Criptografia – AES

Numa proposta de substituir o DES (Data Encryption Standard), o NIST promoveu uma competição para que fosse feito um algoritmo que seria chamado AES (Advanced Encryption Standard) que atendesse as seguintes especificações:

- Algoritmo publicamente definido
- Ser uma cifra simétrica de bloco
- Projetado para que o tamanho da chave possa aumentar
- Implementável tanto em hardware quanto em software
- Disponibilizado livremente ou em acordo com termos ANSI

INSTITUTO FEDERAL
Goiás

Criptografia – AES

Onde o AES foi julgado:

- Segurança (esforço requerido para criptoanálise)
- Eficiência computacional
- Requisitos de memória
- Adequação a hardware e software
- Simplicidade

O processo seletivo teve inicio em 1997 e terminou em 2000 com a vitória do algoritmo Rijndael escrito por Vincent Rijmen e Joan Daemen.

Este algoritmo criptografa e descriptografa usando uma chave criptografada e blocos, ambos de tamanhos de 128, 192 ou 256 bits.

Criptografia – AES

- **Vantagens quanto à implementação:**
  - Pode rodar bem rapidamente em relação a outros algoritmos.
  - Pode ser implementado em um SmartCard usando pouco código e memória.
  - Algumas funções podem ser feitas em paralelo, assim tornando o processo mais rápido.
  - Como a encriptação não emprega operações aritméticas, não exige muito poder de processamento.

Criptografia – AES

- **Vantagens quanto à simplicidade do projeto:**
  - Não usa elementos já previamente processados, por ex. a 9a rodada não necessita de nenhum elemento das rodadas anteriores a não ser única e exclusivamente do *estado* da 8a.
  - 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.

Criptografia – AES

- **Vantagens quanto à possíveis modificações:**
  - O projeto permite a especificação de variantes com o comprimento do bloco e da chave, ambos variando de 32 em 32 bits no intervalo de 128 até 256 bits.
  - Embora o número das rodadas seja fixo na especificação, pode ser modificado como um parâmetro caso haja problemas de segurança.

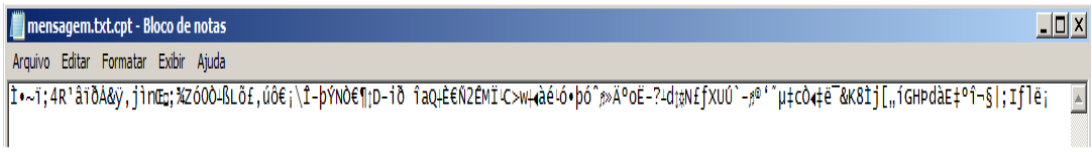
Criptografia – AES

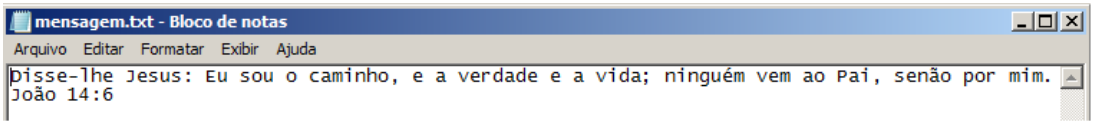
- **As Desvantagens ficam por conta da inversa:**
  - A inversa é menos recomendável de ser implementada num SmartCard, pois precisa de mais código e mais processamento. Mesmo assim, se comparado, a outros algoritmos ela bem rápida.
  - Em software, a encriptação e sua inversa empregam códigos diferentes e/ou tabelas.
  - Em hardware a inversa pode usar apenas uma parte do circuito usado no processo de encriptação.

INSTITUTO FEDERAL
Goiás

Criptografia – AES

Mensagem criptografada utilizando o comando “ccrypt”:





INSTITUTO FEDERAL
Goiás

Criptografia – Chave Assimétrica

Figura 2. Chave assimétrica

Agora o que muitos realmente confundem é quanto a força bruta dos algoritmos assimétricos! É muito, mas muito diferente!

Em um simétrico, se eu tenho 8 bits de chave, tenho 256 combinações possíveis.

Se pegar o caso do RSA que é um assimétrico e se tiver uma chave de 8 bits, significa que o valor do N é de 256 bits. Sem querer descrever o RSA aqui, podemos dizer que N é o resultado da multiplicação de dois números primos de 4 bits. Quebrar a chave significa achar um destes números. E não é de 2^4 tentativas, pois os valores 2, 4, 6, 8, 9, 10 não precisam ser testados pois não são primos!

No universo de 4 bits só existem estes primos: 2, 3, 5, 7, 11 e 13. Só isso! Mata-se em seis tentativas no máximo!

Criptografia – Chave Assimétrica

Para algoritmos assimétricos, como no caso do RSA, o cálculo do esforço matemático não é simplesmente de 2^B (B = Número de bits). É muito, mas muito menos que isto.

Exatamente por isto é que os algoritmos assimétricos precisam de uma chave muito maior, hoje perto dos 1024 bits. No caso do RSA, dizer que ele é de 1024 bits, significa que o valor de N é de 1024 bits, logo, quebrar significa encontrar um número primo de até 512 bits que sirva.

Aí tem gente que se acostumou a ver o RSA de 1024 bits e sai dizendo que um AES de 128 é fraco, pois são só 128 bits! Porém, são coisas muito diferentes!

INSTITUTO FEDERAL
Goiás

Criptografia – PGP

- **Definição do PGP:** PGP, do inglês Pretty Good Privacy (Privacidade Muito Boa), é um programa de computador de encriptação e descriptografia de dados (criptografia de chave assimétrica) que fornece autenticação e privacidade criptográfica para comunicação de dados.

- **Histórico do PGP:** O PGP foi criado no início da década de 90 e muitas vezes é confundido como um algoritmo de criptografia, um conceito equivocado. O PGP é um software inicialmente desenvolvido por Phil Zimmermann nos Estados Unidos, que adaptou conceitos já existentes da criptografia, no intuito de criar um sistema de fácil utilização,possibilitando até mesmo para uma pessoa comum a utilização da criptografia em seu dia a dia, desde que tivesse em mãos um computador.

INSTITUTO FEDERAL
Goiás

Criptografia – PGP

- **Definição do PGP:** PGP, do inglês Pretty Good Privacy (Privacidade Muito Boa), é um programa de computador de encriptação e descriptografia de dados (criptografia de chave assimétrica) que fornece autenticação e privacidade criptográfica para comunicação de dados.

- **Histórico do PGP:** O PGP foi criado no início da década de 90 e muitas vezes é confundido como um algoritmo de criptografia, um conceito equivocado. O PGP é um software inicialmente desenvolvido por Phil Zimmermann nos Estados Unidos, que adaptou conceitos já existentes da criptografia, no intuito de criar um sistema de fácil utilização,possibilitando até mesmo para uma pessoa comum a utilização da criptografia em seu dia a dia, desde que tivesse em mãos um computador.

INSTITUTO FEDERAL
Goiás

Criptografia – PGP

- Problema com o governo dos EUA
- Zimmermann publicou um livro com o código fonte do PGP
- Zimmermann respondeu a vários processos e acabou inocentado
- PGP acabou se transformando em um software fechado
- Em 1998, a PGP Corporation lança o OpenPGP
- Os dois softwares (PGP e OpenPGP) se diferenciam pelo suporte, algoritmos de criptografia e transparência
- Em 1999, a Free Software Foundation desenvolveu o GNU Privacy Guard (GPG), o padrão atualmente para PGP, possui diversas interfaces gráficas (Seahorse, Kleopatra, Mailvelope, Enigmail, GPA, etc).

INSTITUTO FEDERAL
Goiás

Criptografia – PGP

Os três pilares do PGP:

- **Confidencialidade:** Visa garantir que ninguém que não possua as chaves criptográficas possa visualizar o conteúdo de uma determinada mensagem. Esse pilar define o segredo que a mensagem cifrada se torna ao esconder o texto simples. Não é difícil que uma mensagem seja interceptada durante a sua transmissão, o PGP deve impedir que o conteúdo da mesma seja inteligível para quem não deve.
- **Integridade:** Este pilar estabelece de que uma mensagem não sofrerá alterações durante a sua transmissão, a forma que ela foi enviada será exatamente a forma que ela será recebida. O sistema OpenPGP possui um mecanismo de notificação que avisa o destinatário caso a mensagem tenha sofrido alguma alteração após o seu envio.

Criptografia – PGP

- **Não repúdio:** Este fundamento procura evitar que uma mensagem recebida com a assinatura digital do remetente não possa ser negada por ele, em outras palavras, a partir do momento em que se assina digitalmente uma mensagem com uma chave privada, está sendo comprovado de que o remetente da mensagem é a mesma pessoa que a escreveu, e ela não pode repudiar este fato. É recomendável que as mensagens cifradas sempre sejam assinadas digitalmente para prevenir possíveis tentativas de envio de mensagens falsas.
- **Autenticidade:** A união dos três pilares descritos acima, se aplicada de forma correta numa transmissão de mensagem, garante a autenticidade da mesma, ou seja, o destinatário pode ter certeza de que foi alguém conhecido que lhe enviou a mensagem, através da assinatura, pode comprovar que a mensagem não foi vista em sua transmissão ou adulterada.

INSTITUTO FEDERAL
Goiás

Criptografia – PGP

O PGP é muito utilizado em mensagens enviadas via e-mail, tanto que boa parte de seus softwares derivados possuem plugins para se adaptarem aos gerenciadores de e-mail de seus usuários.

É o caso do Mailvelope - https://www.mailvelope.com/ - que usaremos numa demonstração a seguir.

INSTITUTO FEDERAL
Goiás

Criptografia – Bibliografia

- https://www.vivaolinux.com.br/artigo/Introducao-a-criptografia?pagina=6
- https://pt.wikipedia.org/wiki/Advanced_Encryption_Standard
- http://dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/edilson_fernandes.pdf
- http://rabci.org/rabci/sites/default/files/Artigo_Criptografia.pdf
- https://pt.wikipedia.org/wiki/OpenPGP