Segurança de Redes de Computadores

Ricardo José Cabeça de Souza

www.ricardojcsouza.com.br

ricardo.souza@ifpa.edu.br

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Criptografia

- **CRC (*Cyclic Redundancy Check)***
  - Verificação de redundância cíclica
  - É um código detector de erros
  - Tipo de função hash que gera um valor expresso em poucos bits em função de um bloco maior de dados, como um pacote de dados, ou um arquivo

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Criptografia

- **CRC (*Cyclic Redundancy Check)***
  - Objetivo é detectar erros de transmissão ou armazenamento
  - CRC é calculado e anexado à informação a transmitir (ou armazenar) e verificado após a recepção ou acesso, para confirmar se não ocorreram alterações

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Criptografia

- **CRC (*Cyclic Redundancy Check)***
  - É calculado através das operações da aritmética módulo 2
  - É o resto da divisão polinomial entre os dados a enviar, e um polinômio gerador adequadamente escolhido
  - Polinômios geradores padronizados
  - cada posição dos bits no bloco de dados ou arquivo é considerado como uma potência de ***x*** no polinômio

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Criptografia

- **CRC (*Cyclic Redundancy Check)***
  - Exemplo, a sequencia de bits 1001101100110100 deve ser considerada como sendo o polinômio:

$$P(x) = 1x^{15} + 0x^{14} + 0x^{13} + 1x^{12} + 1x^{11} + 0x^{10} + 1x^{9} + 1x^{8} + 0x^{7} + 0x^{6} + 1x^{5} + 1x^{4} + 0x^{3} + 1x^{2} + 0x^{1} + 0x^{0}$$

ou seja:

$$P(x) = x^{15} + x^{12} + x^{11} + x^{9} + x^{8} + x^{5} + x^{4} + x^{2}$$

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Criptografia

- **CRC (*Cyclic Redundancy Check)***
  - Polinômios geradores padronizados

$$CRC_{32}(x) = x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^{8}+x^{7}+x^{5}+x^{4}+x^{2}+x^{1}+x^{0}$$

$$CRC_{16}(x) = x^{16} + x^{15} + x^{2} + x^{0}$$

$$CRC_{12}(x) = x^{12} + x^{3} + x^{1} + x^{0}$$

$$CRC_{8}(x) = x^{8} + x^{2} + x^{1} + x^{0}$$

$$CRC_{1}(x) = 1$$

Criptografia

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

- **CRC (*Cyclic Redundancy Check)***
  - Exemplo de Cálculo do CRC
  - **TRANSMISSOR:**
  - Mensagem(M): 111100101
    - Multiplicar M(x) por $\mathbf{X^r}$ – **r** maior expoente de G(x)
      - M(x)=$\mathbf{X^8+X^7+X^6+X^5+X^2+1}$ * $\mathbf{X^5}$ = $X^{13}+X^{12}+X^{11}+X^{10}+X^7+X^5$
    - M(x) = **111100101000000**
    - Polinômio de M(x)=$X^{13}+X^{12}+X^{11}+X^{10}+X^7+X^5$
  - Polinômio Gerador(G): 101101
    - G(x)=$X^5+X^3+X^2+1$
  - Divisão(Módulo 2) da Mensagem pelo Gerador
    - Resto(5 bits): $\mathbf{X^3+X}$ → 1010 → **01010 (5 bits)**
    - Mensagem a ser transmitida
    - T(x) = **111100101**01010

Criptografia

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

- **CRC (*Cyclic Redundancy Check)***
  - Exemplo de Cálculo do CRC
  - **RECEPTOR:**
    - Mensagem Recebida(Rx): **11110010101010**
    - $R(x)=X^{13}+X^{12}+X^{11}+X^{10}+X^{7}+X^{5}+X^{3}+X$
    - Polinômio Gerador(G): 101101
    - $G(x)=X^{5}+X^{3}+X^{2}+1$
  - Divisão(Módulo 2) da Mensagem Recebida pelo Gerador
    - Se o Resto = 0 → Recebido sem erro

Criptografia

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

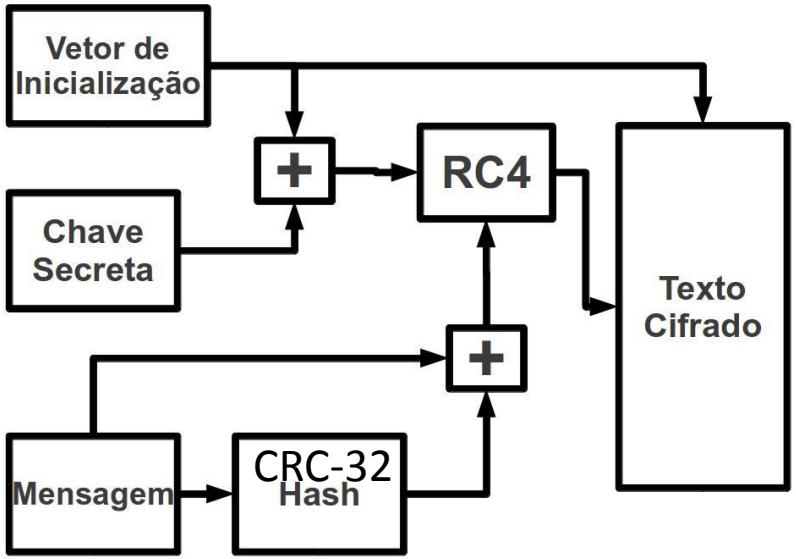
- **WEP Encapsulation Process**
  - Chave WEP é concatenado com um Vetor de Inicialização (IV)
  - Chave combinada é utilizada como semente para um keystream RC4 que é XOR com os dados de WLAN
  - Um fluxo de **IV** diferente é usado para cada quadro, e, portanto, uma chave combinada diferente é utilizado para criar um novo keystream RC4 para cada quadro
  - Vulnerabilidades foram expostos nos Vetores de Inicialização repetidos

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

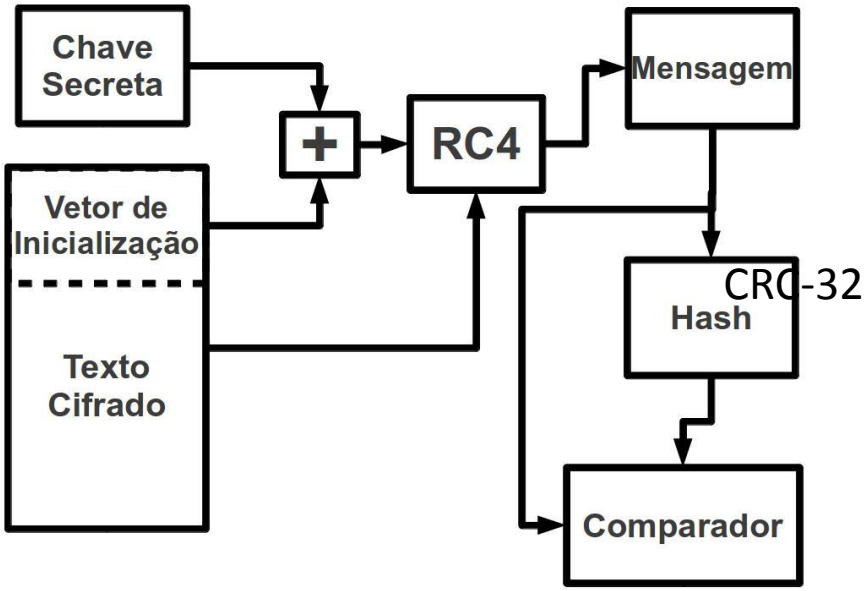
www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Criptografia

- **WEP Encapsulation Process**



ENCRIPTAÇÃO



DESENCRIPTAÇÃO

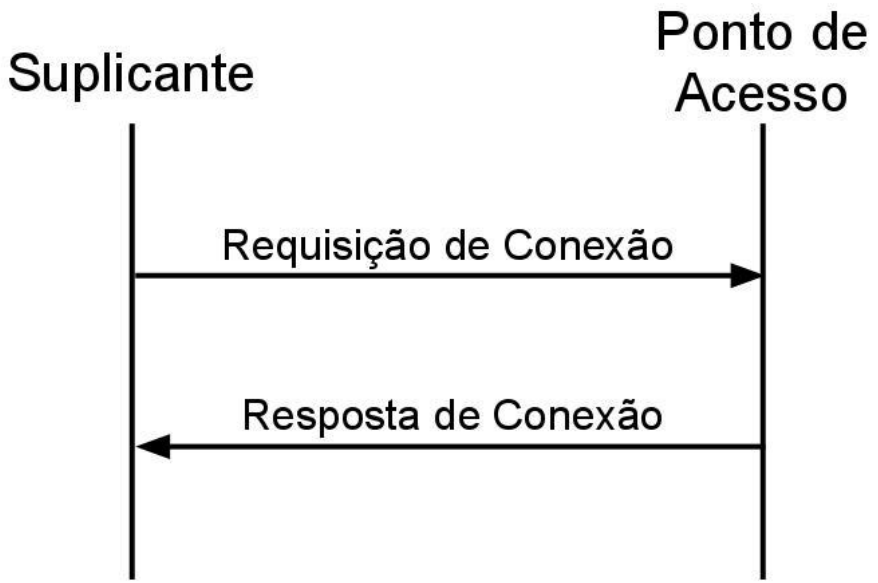
Fonte da Imagem: http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2011_2/rodrigo_paim/images/wep_1.jpg

Fonte da Imagem: http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2011_2/rodrigo_paim/images/wep_2.jpg

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Criptografia

- **WEP Encapsulation Process**
  - Processo de Autenticação - Modos:
    - Sistema aberto ("Open System")
      - Qualquer um que conheça o SSID(Service Set Identifier) é passível de se identificar

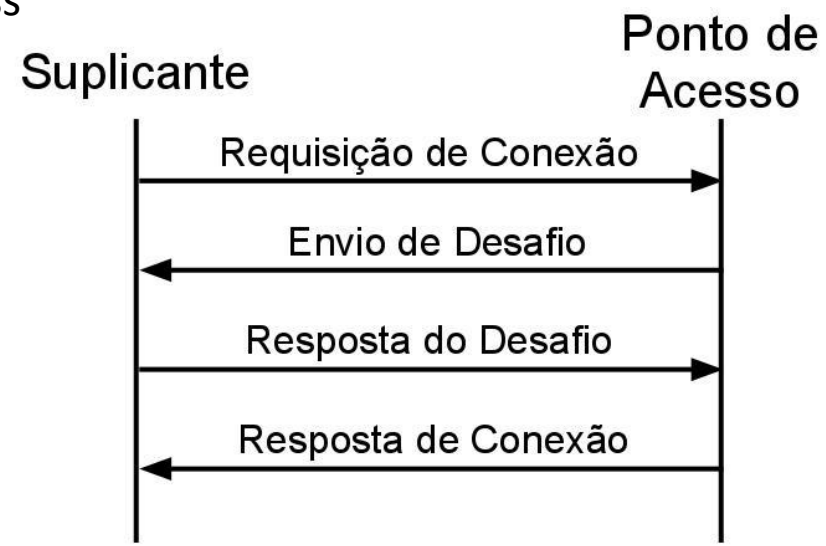


Fonte da imagem: http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2011_2/rodrigo_paim/images/wep_3.jpg

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Criptografia

- **WEP Encapsulation Process**
  - Processo de Autenticação - Modos:
    - Chave compartilhada ("Shared Key")
      - Só realiza a conexão de quem possuir a chave secreta que o access point possui
      - Ponto de acesso envia uma mensagem com um desafio
        - » Número inteiro aleatório
        - » Máquina responde mensagem contendo este número encriptado de acordo com o processo encriptação



Fonte da Imagem: http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2011_2/rodrigo_paim/images/wep_4.jpg

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Criptografia

- **WEP Encapsulation Process**
  - **Falhas:**
    - *Força Bruta*
      - Chave secreta do WEP possui 40 bits
      - Valor relativamente alto, mas que, com o uso de ataques de dicionário, isto é, através da utilização de nomes que são comumente utilizados, torna-se plausível sua descoberta

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Criptografia

- **WEP Encapsulation Process**
  - **Falhas:**
    - *Conexão*
      - Durante a conexão de um suplicante ao ponto de acesso, o desafio passa em claro e logo depois encriptado
      - É possível ter acesso ao mesmo conteúdo das duas formas, facilitando o processo de obtenção da chave secreta

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Criptografia

- **WEP Encapsulation Process**
  - **Falhas:**
    - *Escuta*
      - Existem outros tipos de ataque que conseguem recuperar a chave secreta a partir da escuta do tráfego por alguns minutos, até que o valor do vetor de inicialização se repita

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Criptografia

- **WPA(W**i-Fi **P**rotected **A**ccess)
  - Criado em 2002 pela WFA (Wi-Fi Alliance)
  - Em 2004, a WFA lançou o sucessor do WPA, o WPA2, após a descoberta de algumas falhas de segurança presentes no TKIP
    - TKIP foi substuído pelo protocolo CCMP → usa AES

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Criptografia

- **TKIP** (***T**emporal **K**ey **I**ntegrity **P**rotocol*)
  - Foi criado em 2002
  - Considerada a primeira tentativa de resolver os problemas do WEP
  - Guarda algumas similaridades com o WEP - utiliza também o algoritmo RC4 modificado para embaralhar os dados
  - Utiliza o tamanho de chaves de 128 bits
  - Dobrou o tamanho do vetor de inicialização
    - Possibilidades de keystreams

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Criptografia

- **TKIP** (***T**emporal **K**ey **I**ntegrity **P**rotocol*)
  - É um algoritmo de criptografia baseado em chaves que se alteram a cada novo envio de pacote
  - Principal característica
    - Frequente mudanças de chaves que garante mais segurança
    - A senha é modificada automaticamente por padrão a cada 10.000 pacotes enviados e recebidos pela sua placa de rede

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

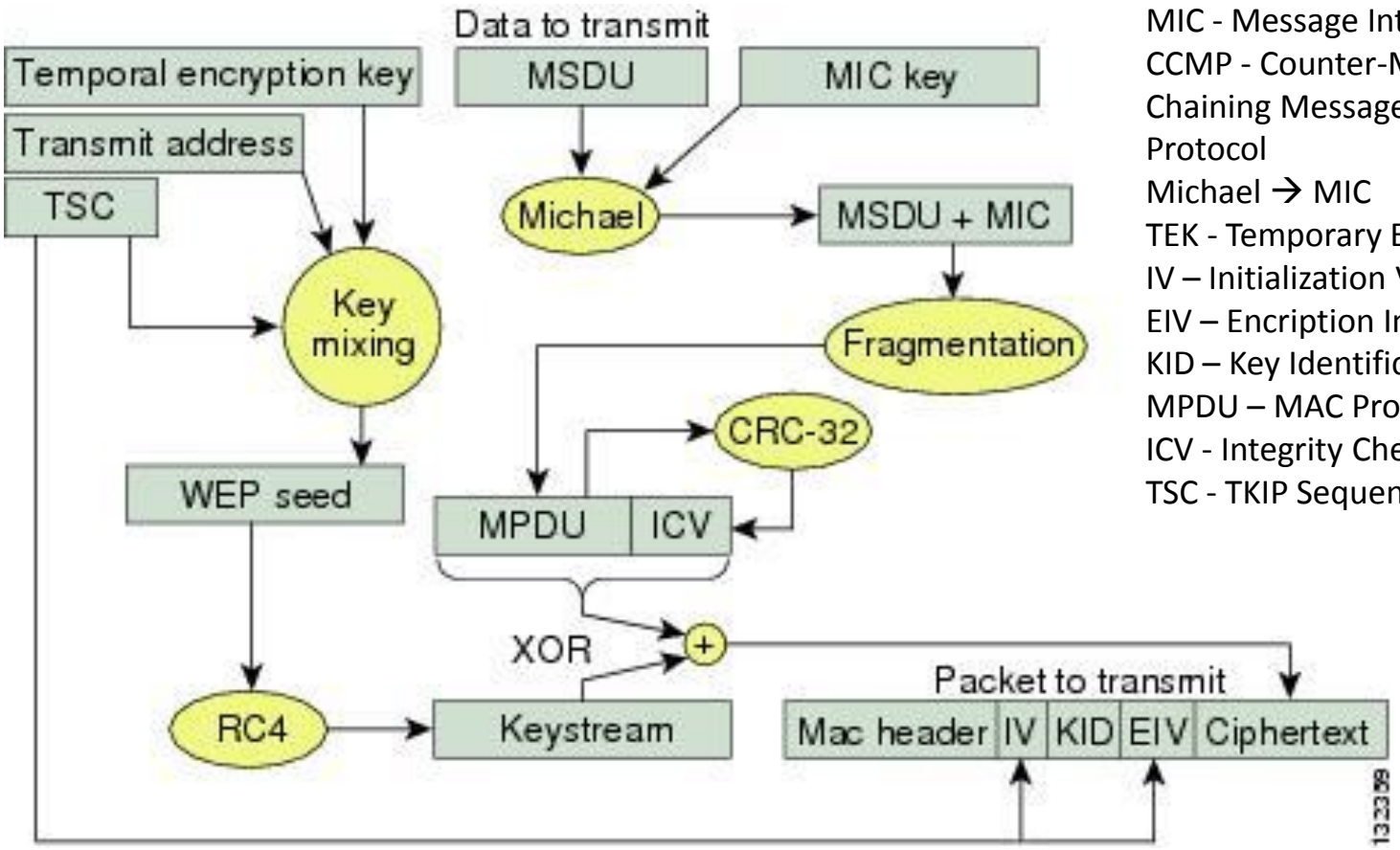
Criptografia

- **TKIP** (***T**emporal **K**ey **I**ntegrity **P**rotocol*)
  - Usa uma combinação entre a chave compartilhada do Ponto de Acesso e do cliente e o endereço MAC do adaptador wireless do cliente
    - Uma nova chave que é gerada fica única e diferente para cada cliente wireless na rede
    - Esta chave resultante é chamada de **Temporal Key**
  - Usado pelo WPA para encriptação da mensagem transmitida

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

Criptografia

- **WPA TKIP**



MSDU - MAC Service Data Unit
MIC - Message Integrity Check
CCMP - Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol
Michael → MIC
TEK - Temporary Encription Key
IV – Initialization Vector
EIV – Encription Initialization Vector
KID – Key Identification
MPDU – MAC Protocol Data Unit
ICV - Integrity Check Value
TSC - TKIP Sequence Counter

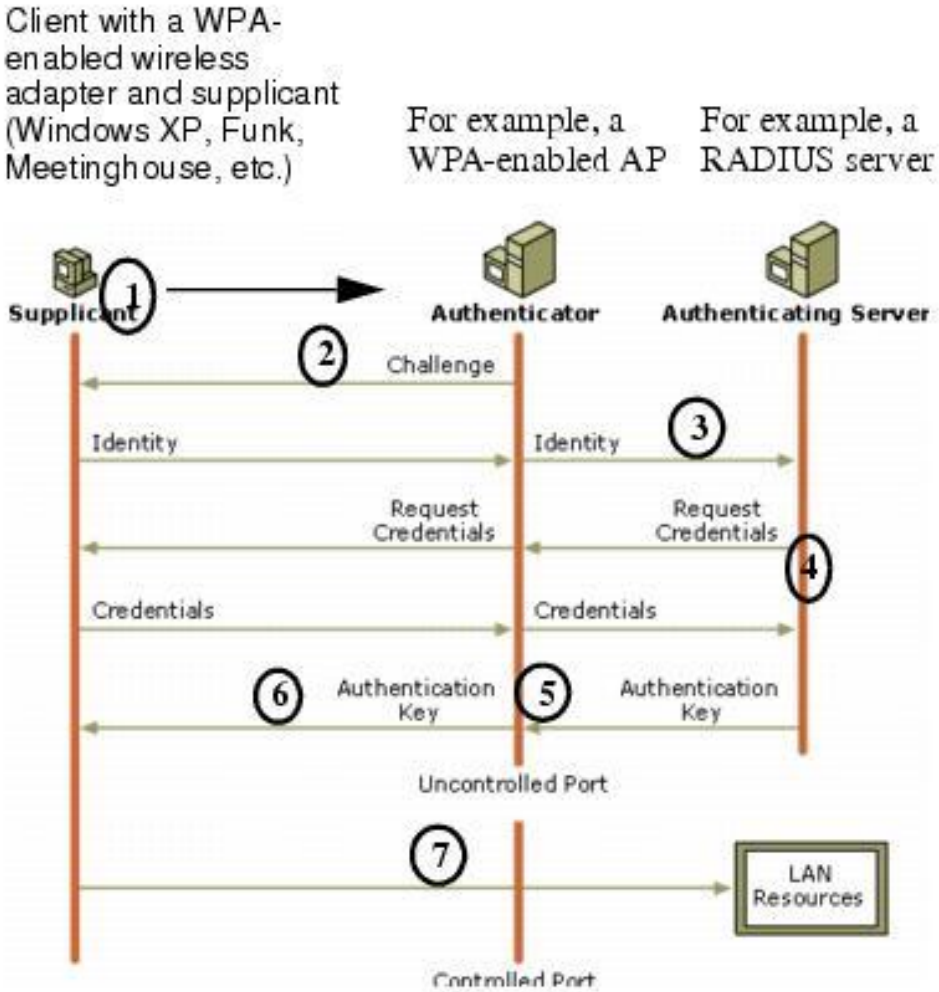
Fonte da Imagem: http://www.cisco.com/en/US/i/100001-200000/130001-140000/132001-133000/132359.jpg

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA PARÁ

Criptografia

- **WPA TKIP**



Fonte da Imagem: http://documentation.netgear.com/reference/fra/wireless/images/8021xAuth.jpg

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PARÁ

Criptografia

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

- **WPA2 AES CCMP**
  - Os dados de autenticação adicional (AAD) é feita a partir do cabeçalho MAC e incluídos no processo de criptografia CCM
  - Isto protege a estrutura contra a alteração das porções não codificados de quadro
  - Para se proteger contra ataques de repetição, uma série de Pacotes Sequenciados (PN) está incluído no cabeçalho CCMP(Counter Mode/CBC MAC Protocol)
  - Os PN e porções do cabeçalho MAC são usados para gerar um uso único que é por sua vez utilizado o processo de encriptação CCM

Referências

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

- STALLINGS, William. **Criptografia e segurança de redes.** 4. ed. São Paulo: Pearson Prentice Hall, 2008.
- FECHINI, Joseana Macêdo. **Segurança da Informação**. Disponível em http://www.dsc.ufcg.edu.br/~joseana/Criptografia-SI.html .
- BRAGA, Hugo Rodrigo. **HISTÓRIA DA CRIPTOLOGIA – Antiguidade**. Disponível em http://www.hu60.com.br/assuntos/criptologia.php .
- Lima, Marcelo. Nakamura, Emílio. **Segurança de Redes e Sistemas**. Versão 1.1.0. Escola Superior de Redes RNP:2007.
- Sousa, Vitor Silva. **Esteganografia**. Disponível em http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2010_2/vitor/Tcnicas.html .
- Disponível em http://www.numaboa.com.br/criptografia/bloco/355-modos-de-operacao .
- **Pretty Good Protocol**. Disponível em http://www.rnp.br/_arquivo/documentos/ref0181.pdf .
- **Protocolo SSH**. Disponível em http://www.gta.ufrj.br/~natalia/SSH/indice.html .

Referências

www.ricardojcsouza.com.br
ricardo.souza@ifpa.edu.br

- Julio, Eduardo Pagani. Brazil, Wagner Gaspar. Albuquerque, Célio Vinicius Neves. **Esteganografia e suas Aplicações.** VII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2007.
- MEDEIROS, Carlos Diego Russo. **SEGURANÇA DA INFORMAÇÃO: Implantação de Medidas e Ferramentas de Segurança da Informação**. Universidade da Região de Joinville – UNIVILLE, 2001.
- NIC BR Security Office. **Cartilha de Segurança para Internet. Parte VII: Incidentes de Segurança e Uso Abusivo da Rede**. Versão 2.0, 2003.
- NIC BR Security Office. **Cartilha de Segurança para Internet. Parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção**. Versão 2.0, 2003.
- FOROUZAN, Behrouz A. **Comunicação de dados e redes de computadores**. 4. ed. São Paulo: McGraw-Hill, 2008.