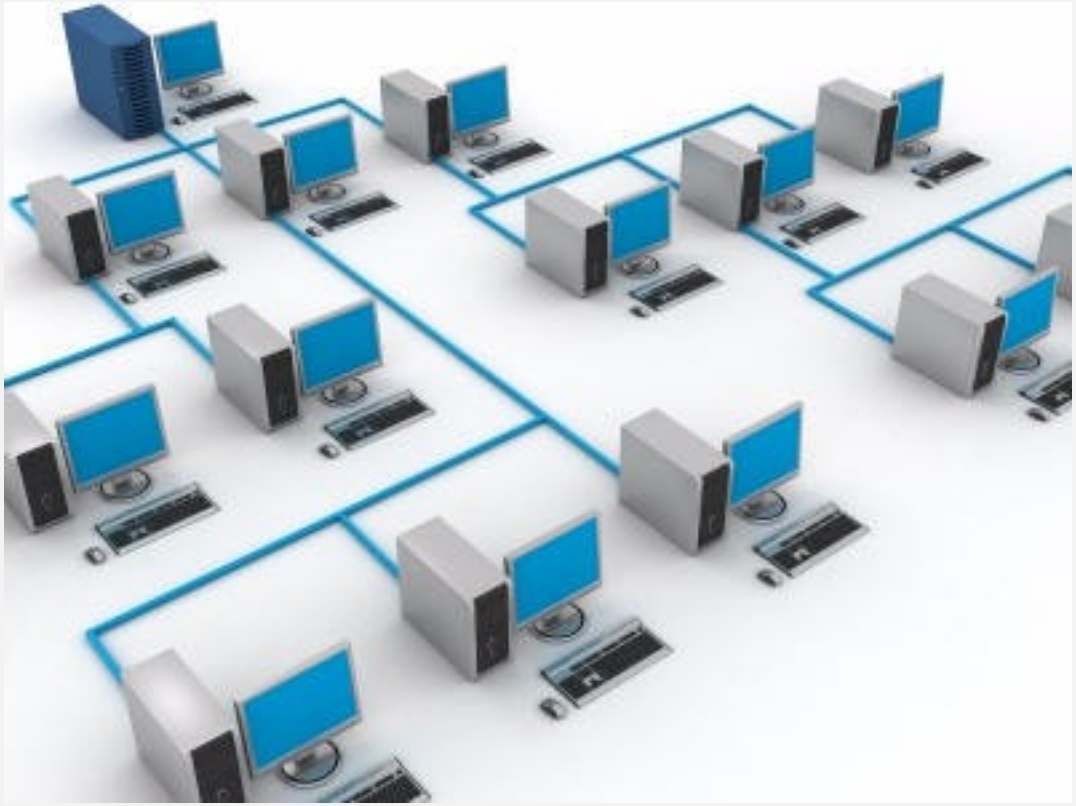
WEP, WPA e EAP

Rodrigo R. Paim

Agenda

- Redes sem Fio e Segurança
- Wired Equivalent Privacy
- Wi-Fi Protected Access
- Extensible Authentication Protocol
- Conclusão

Redes sem Fio e Segurança



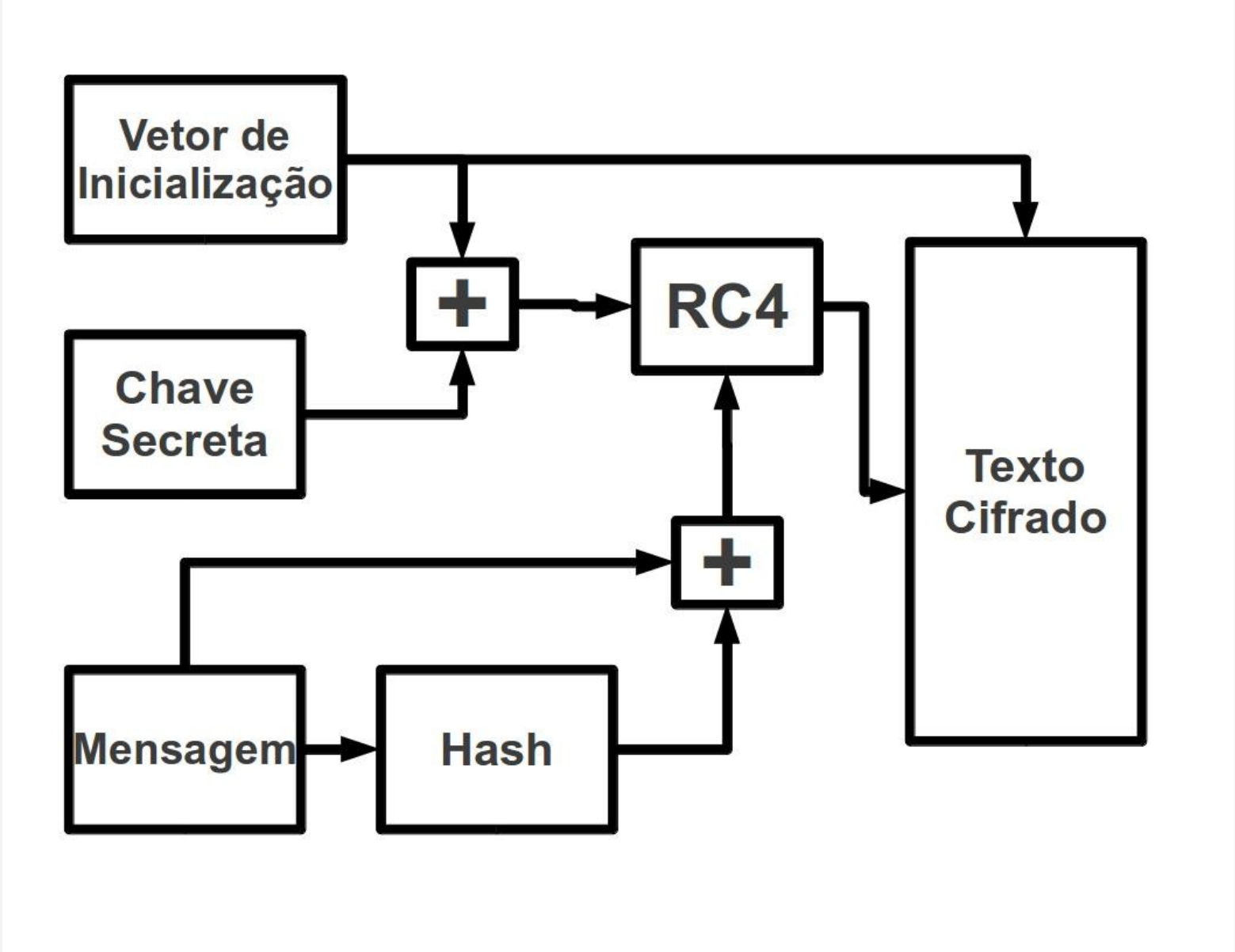
Wired Equivalent Privacy

- Introduzido em 1997
- Autenticação e Encriptação
- Algoritmo de criptografia RC4
- Vetor de Inicialização

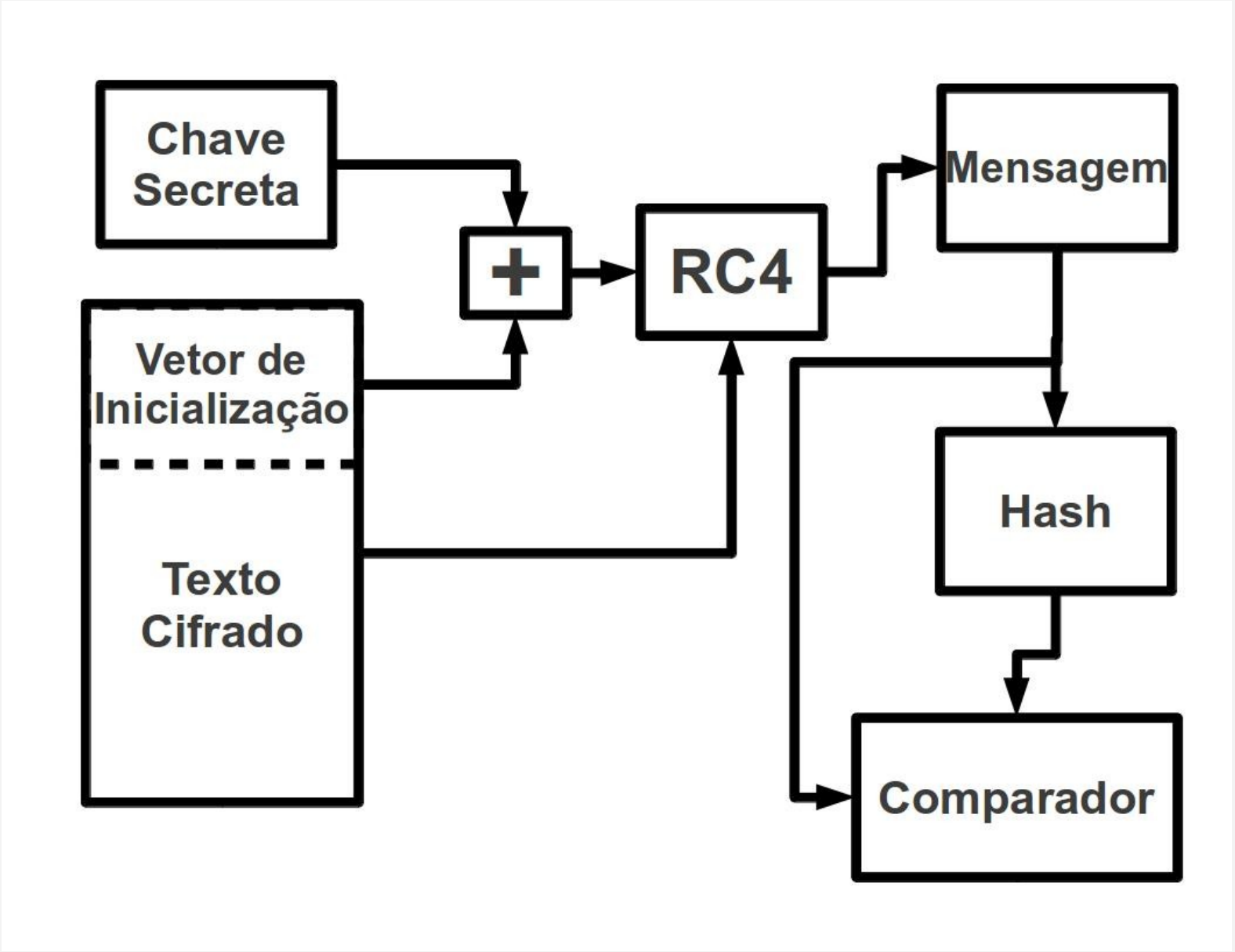
Algoritmo RC4

- Criado por Rivest em 1987
- Cifra de Fluxo
- Algoritmo Escalonador de Chaves
  - Permutação Pseudo-Aleatório da Chave
- Algoritmo de Geração Pseudo-Aleatória
  - XOR entre resultado do KSA e mensagem

WEP - Encriptação



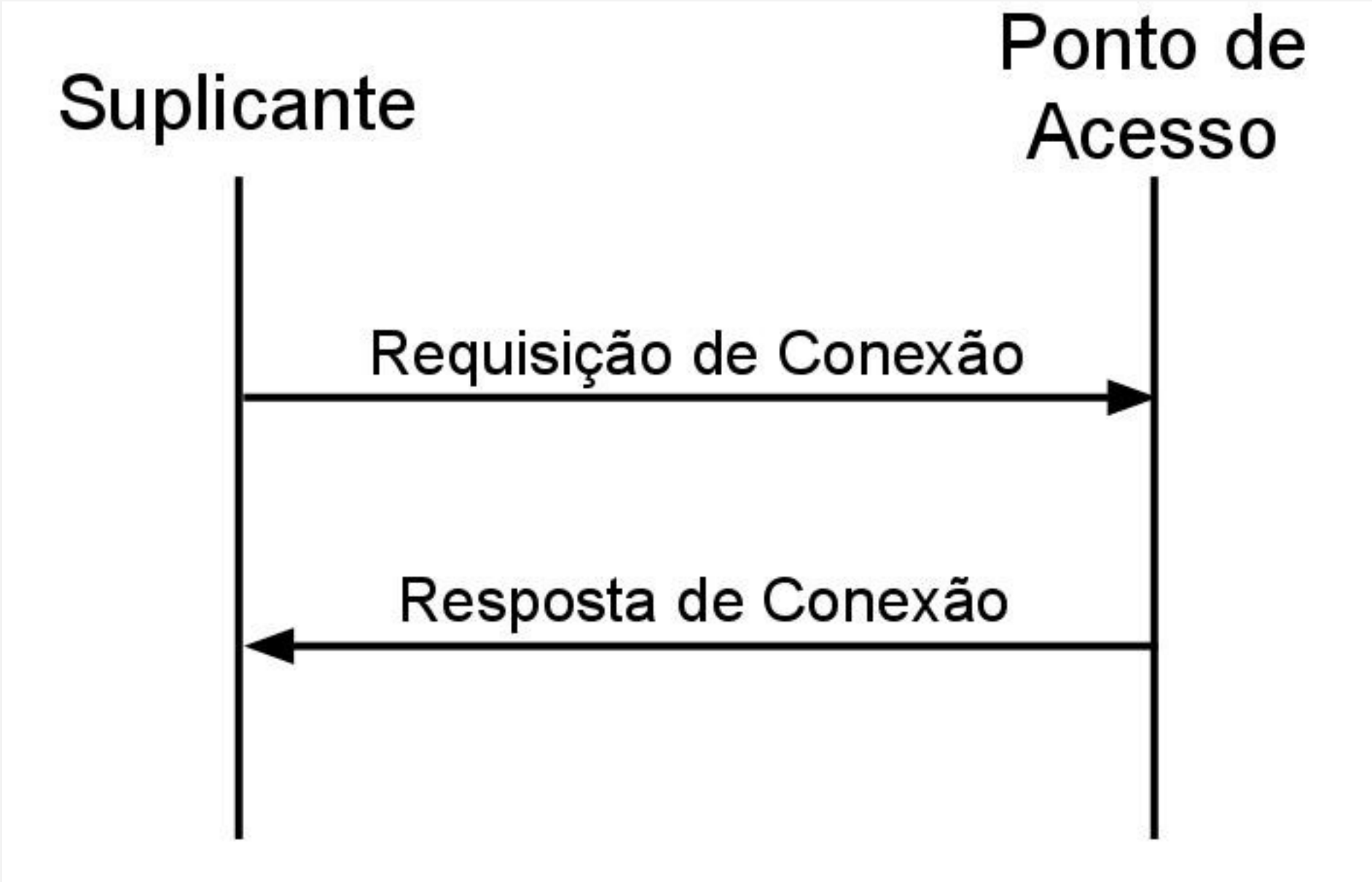
WEP - Decriptação



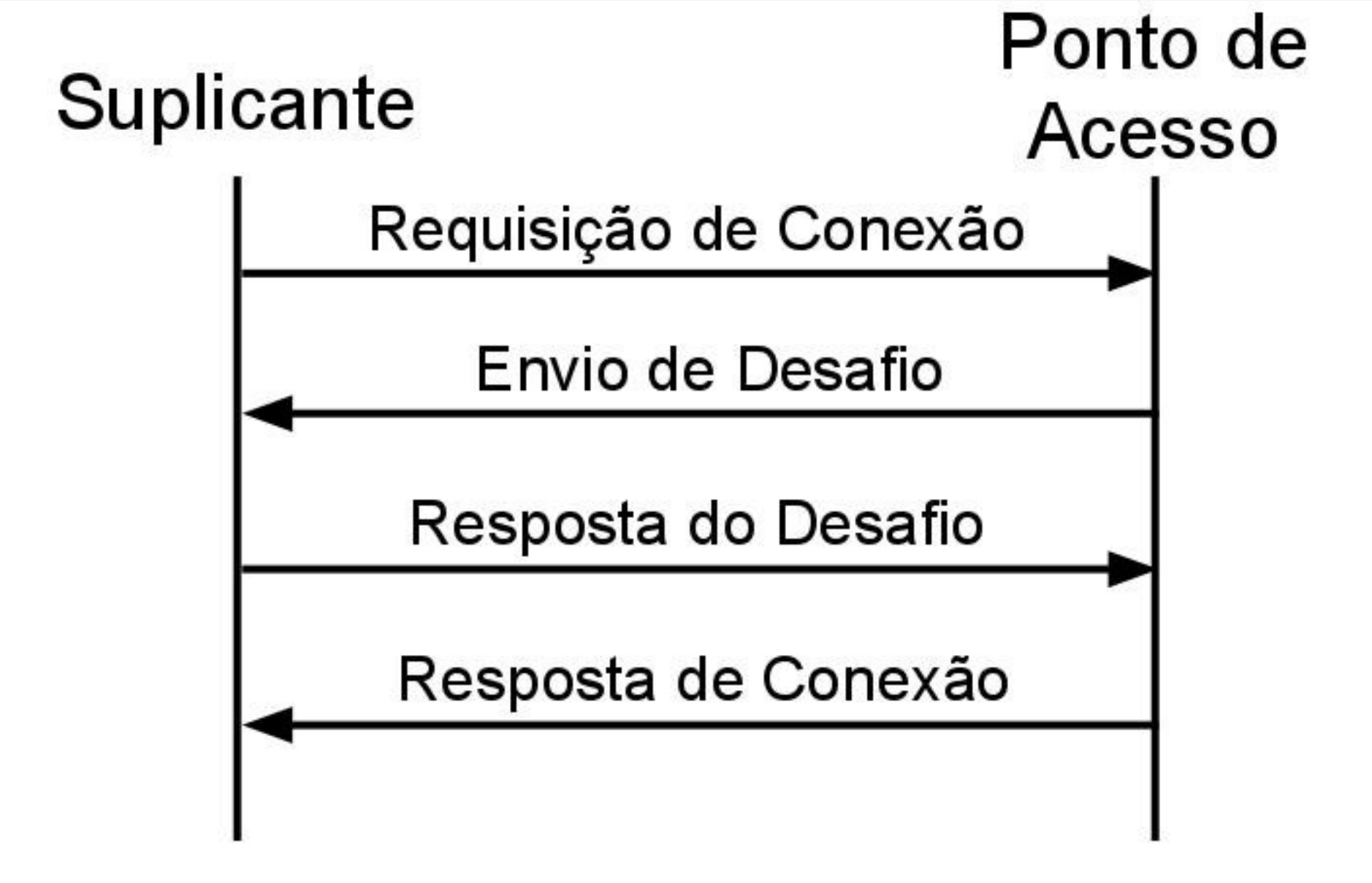
WEP - Autenticação

- Open System
- Shared Key

WEP Open System



WEP Shared Key



Falhas do WEP

- Acesso de Estranhos
  - Força Bruta
  - Conexão
  - Escuta
- Troca de bits
  - Checksum: CRC-32
- Inundação

Evolução do WEP

- WEP2: vetor de inicialização maior
- WEP+: vetor de inicialização inteligente
- WEP Dinâmico: chave periódica

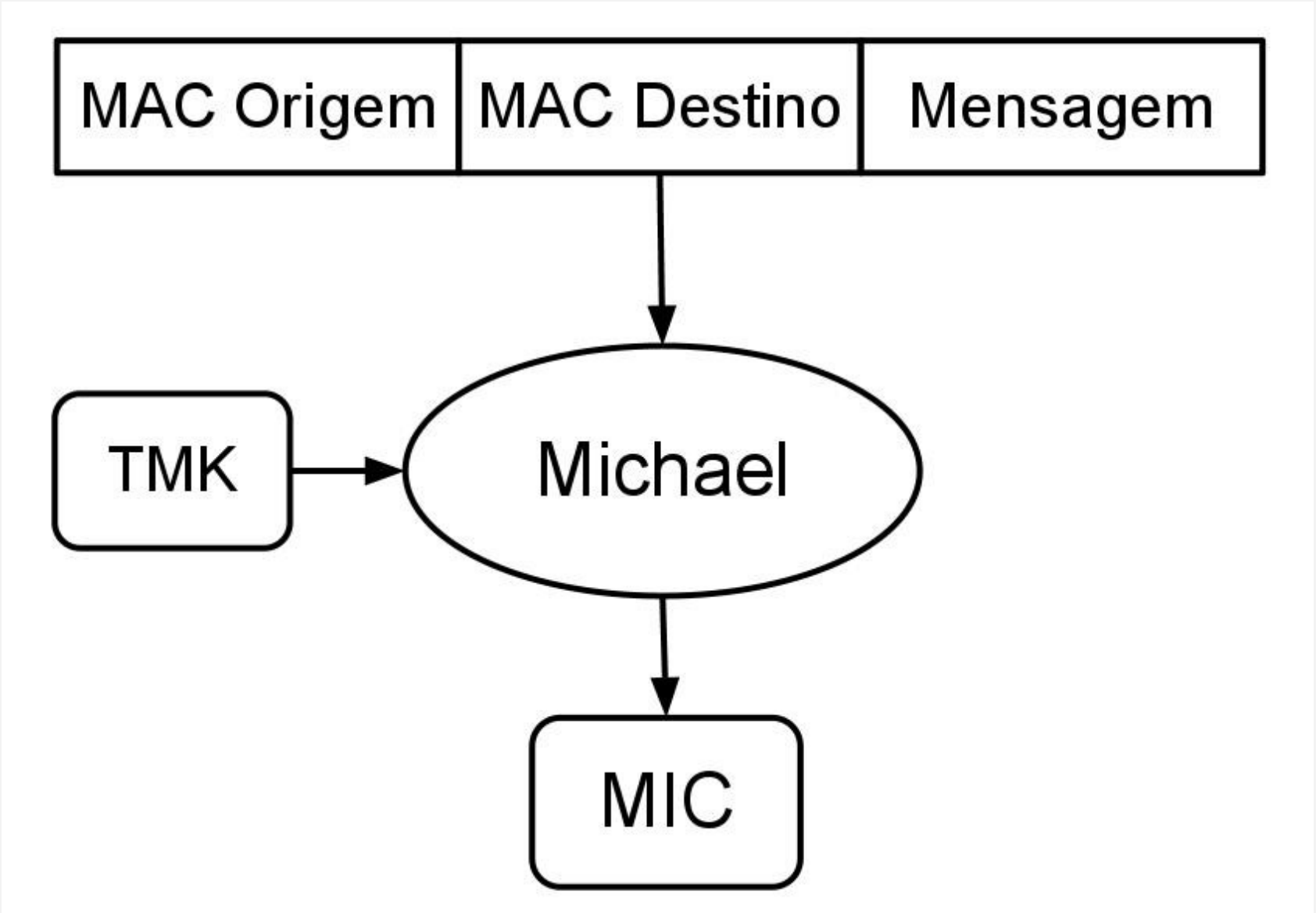
Wi-Fi Protected Access

- Criado em 2002 pela Wi-Fi Alliance
- Correção de falhas do WEP
- Protocolo TKIP: uso do RC4

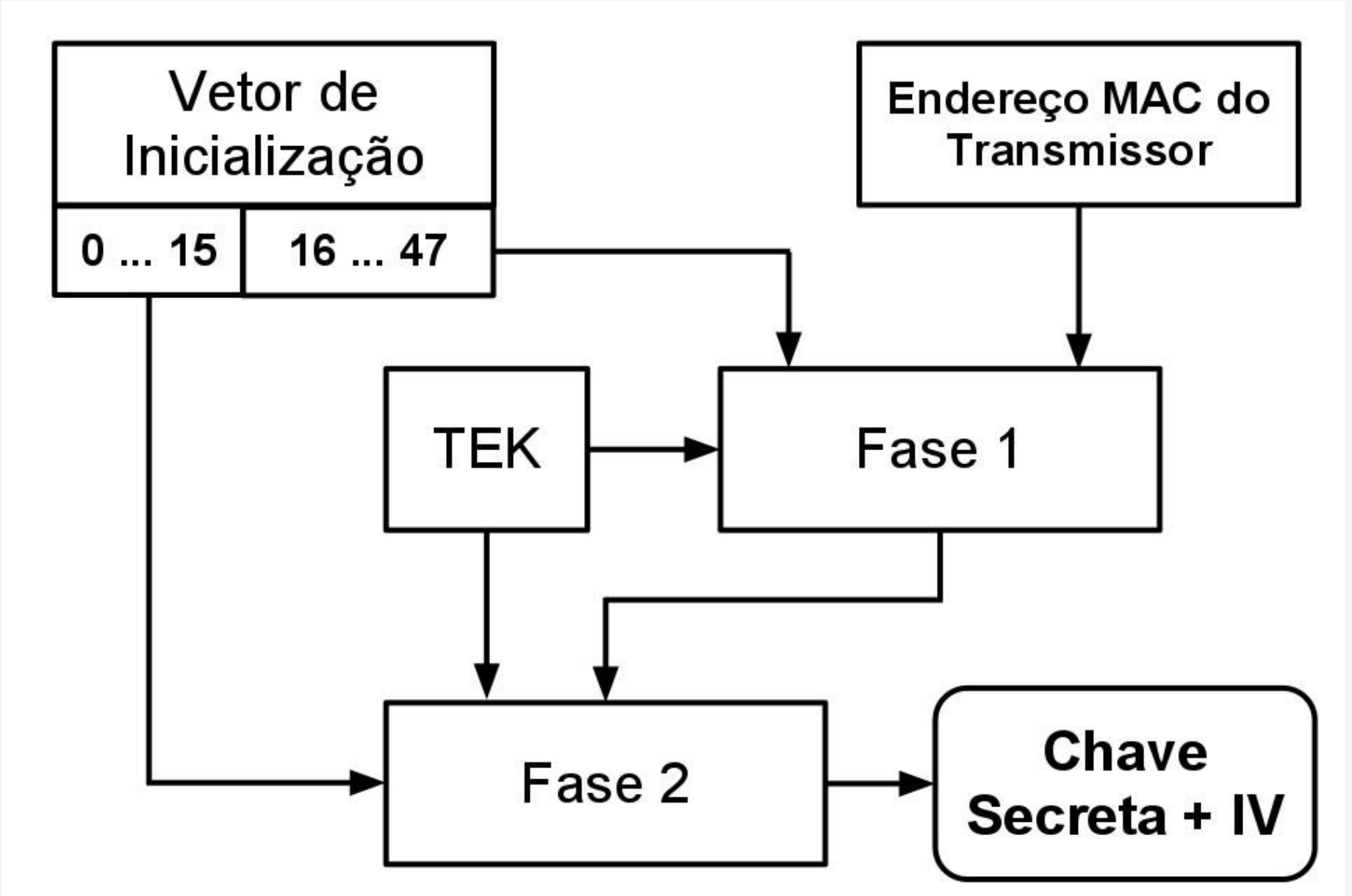
Protocolo TKIP

- P. de Integridade de Chave Temporal
- Chave Mestra PMK
  - Chave Transiente PTK: KCK, KEK, TEK, TMK
- Integridade: MIC
- Vetor de Inicialização crescente
- Encriptação/Decriptação em Fases

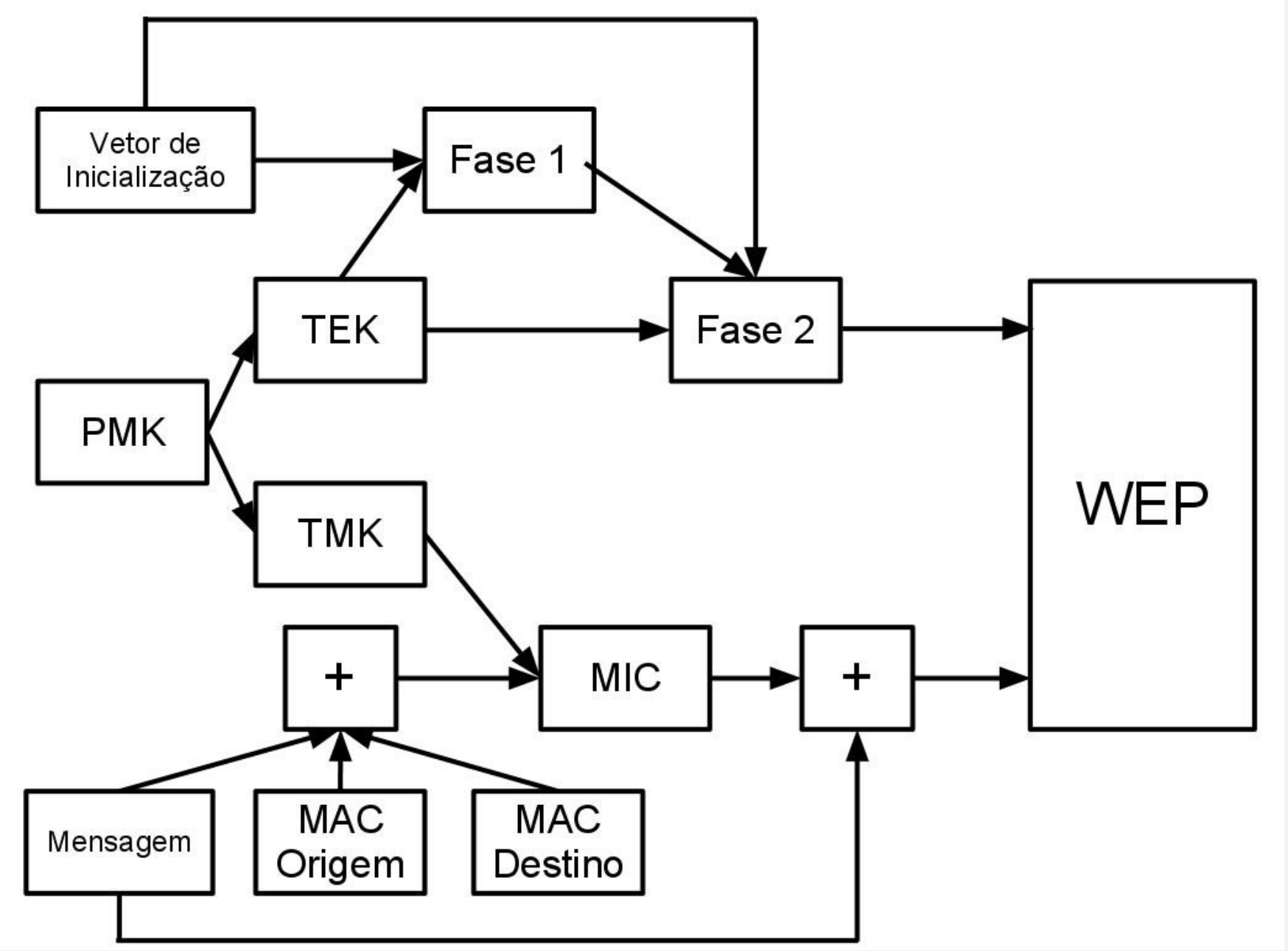
TKIP - Integridade



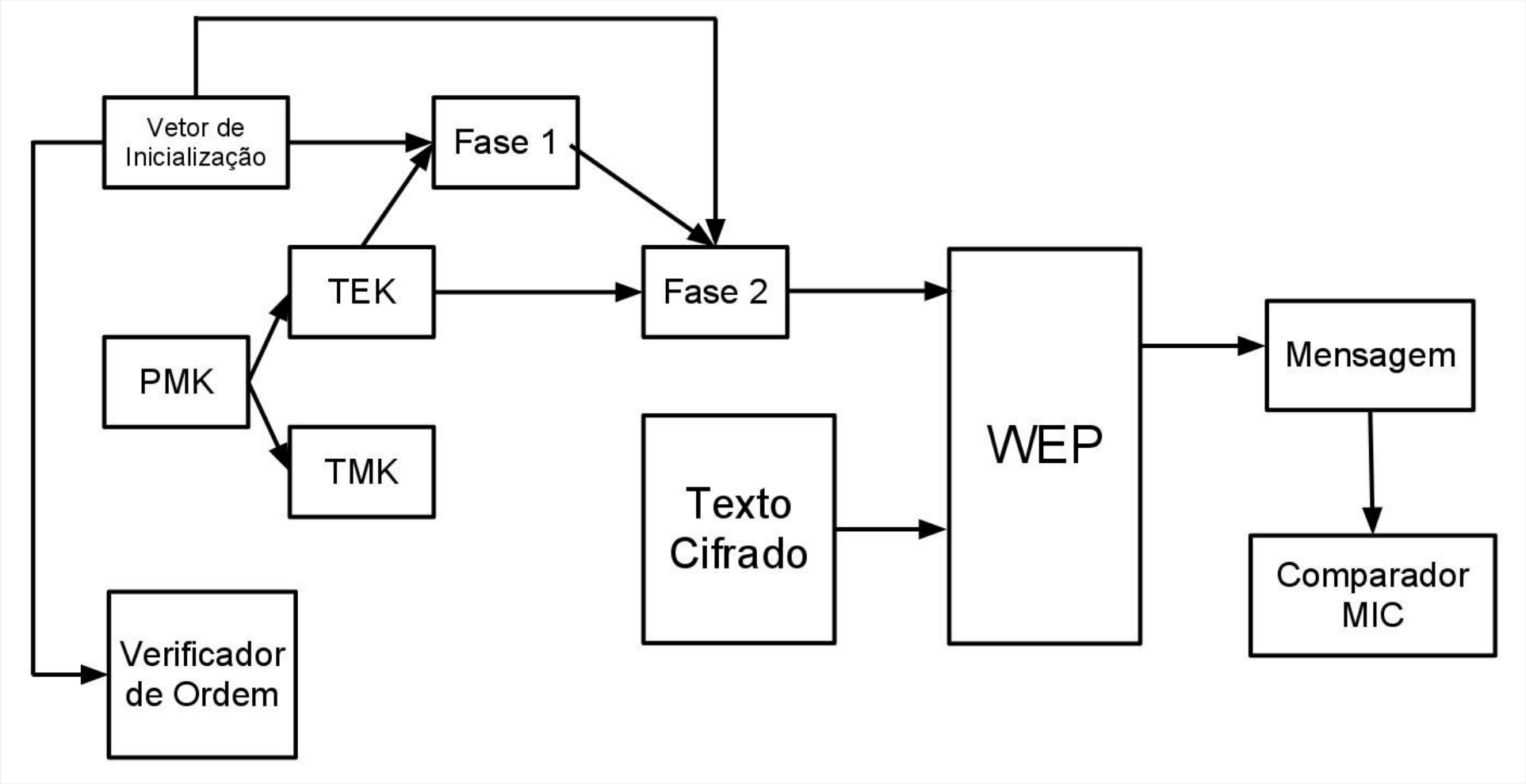
TKIP - Mistura de Chaves



WPA - Encriptação



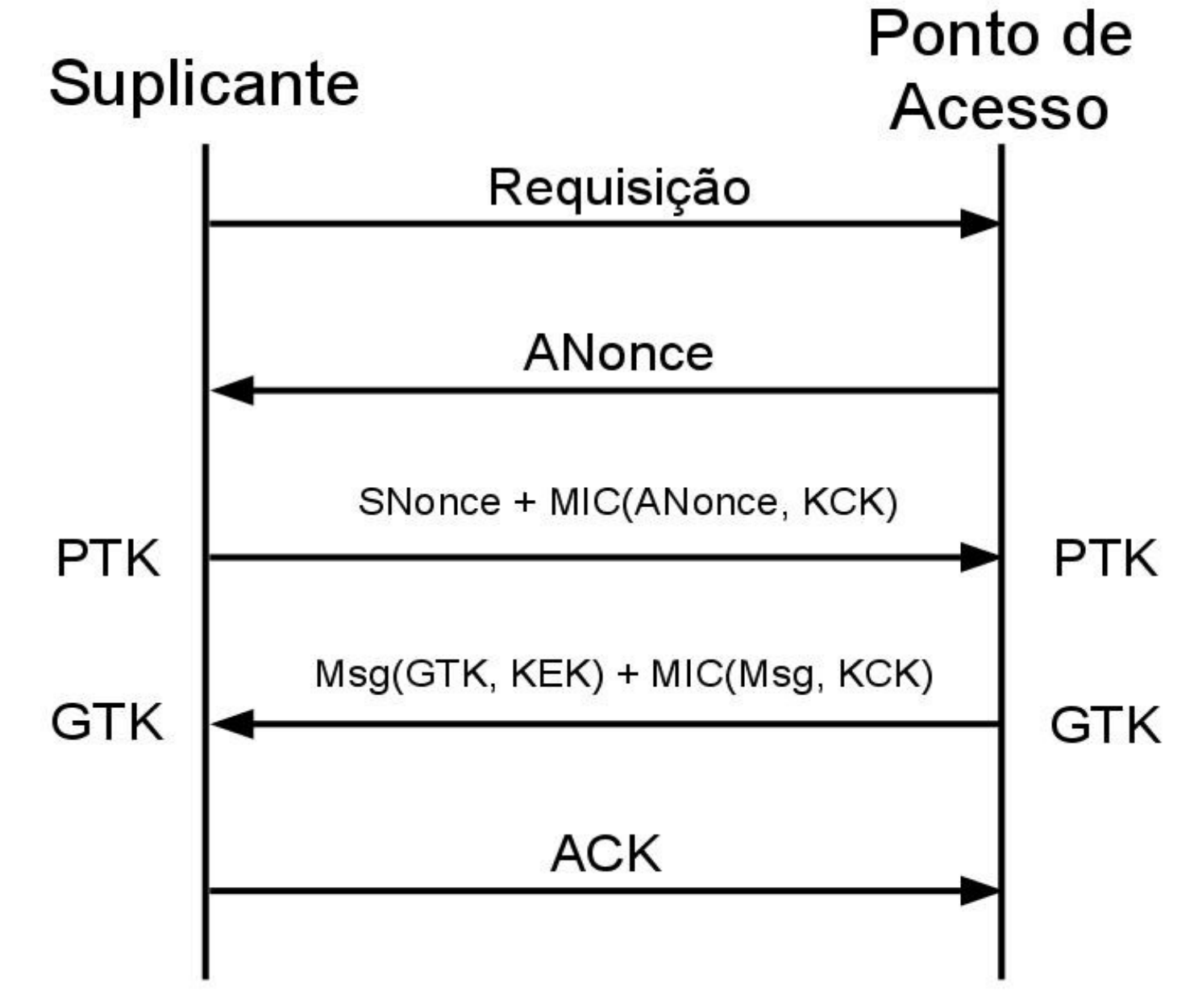
WPA - Decriptação



WPA - Autenticação

- WPA Comercial (depois)
- WPA Pessoal (PSK)
  - Acesso "Unicast e Broadcast"

WPA PSK


Suplicante
Ponto de Acesso
Requisição
ANonce
SNonce + MIC(ANonce, KCK)
PTK
PTK
Msg(GTK, KEK) + MIC(Msg, KCK)
GTK
GTK
ACK

Wi-Fi Protected Access 2

- Lançado em 2004: padrão definitivo
- Abandono do RC4
- Protocolo CCMP
- Algoritmo de Criptografia AES

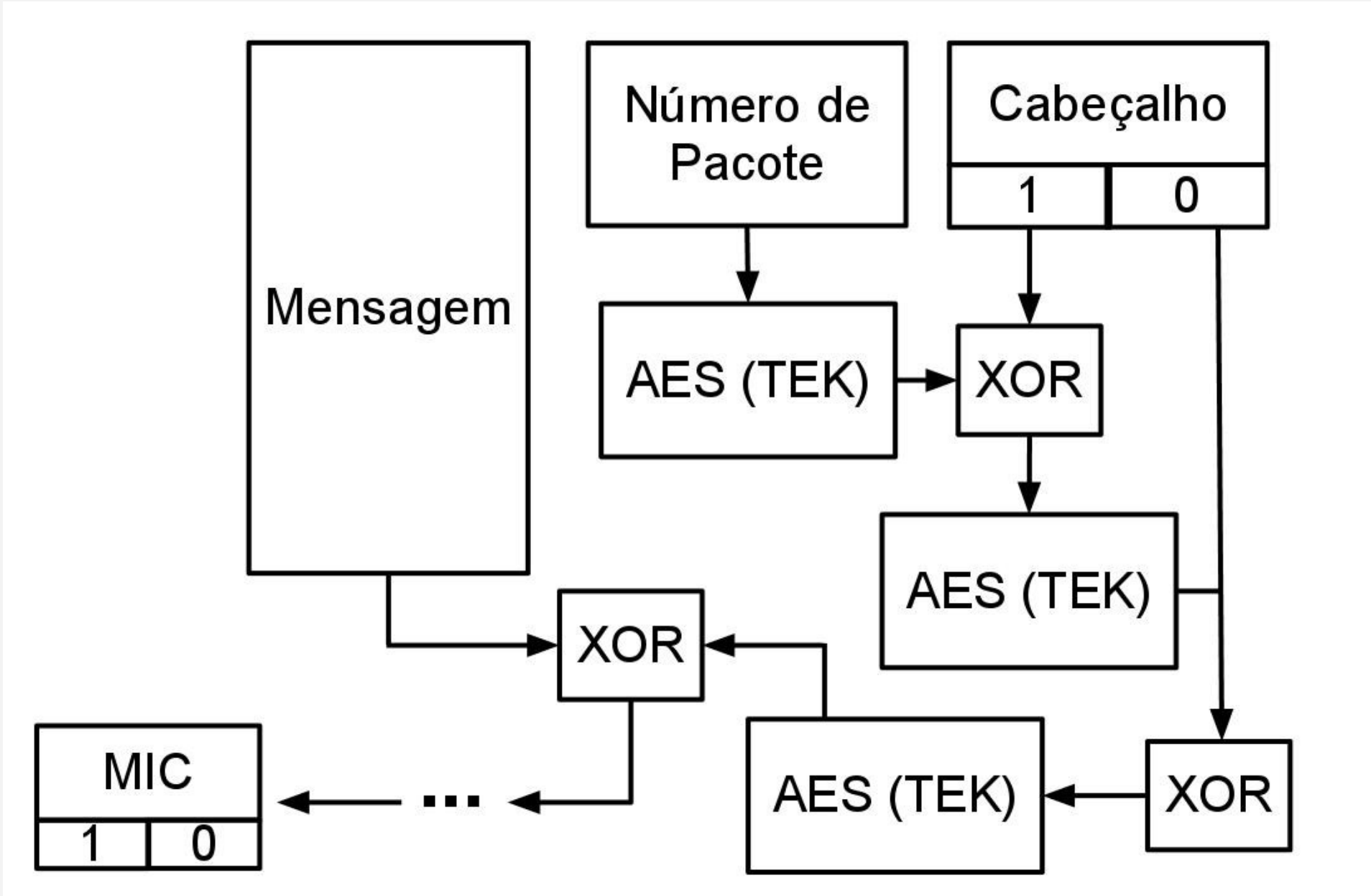
Algoritmo AES

- Padrão de Encriptação Avançado
- Vencedor de concurso do NIST
  - Algoritmo de Rijndael
- Alternativa ao DES
- Criptografia Simétrica de Cifra de Bloco
- Rodadas: permutação e combinação de bits

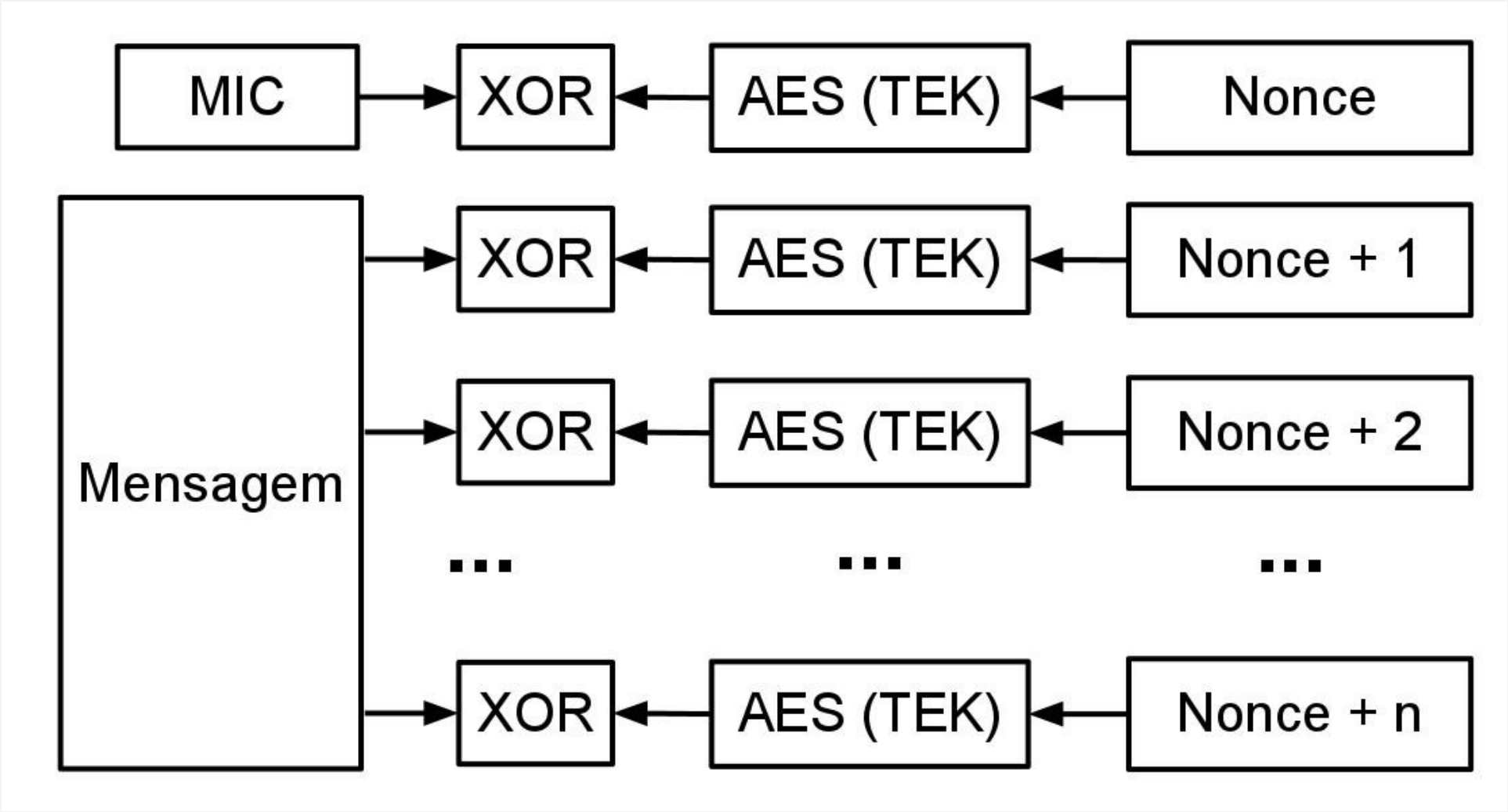
Protocolo CCMP

- Autenticação Análoga ao WPA
- PTK menor: não existe TMK
- Criptografia usando cabeçalho do quadro
- Vetor de Inicialização: Número de Pacote
- Nonce: parâmetros do quadro

CCMP - Integridade



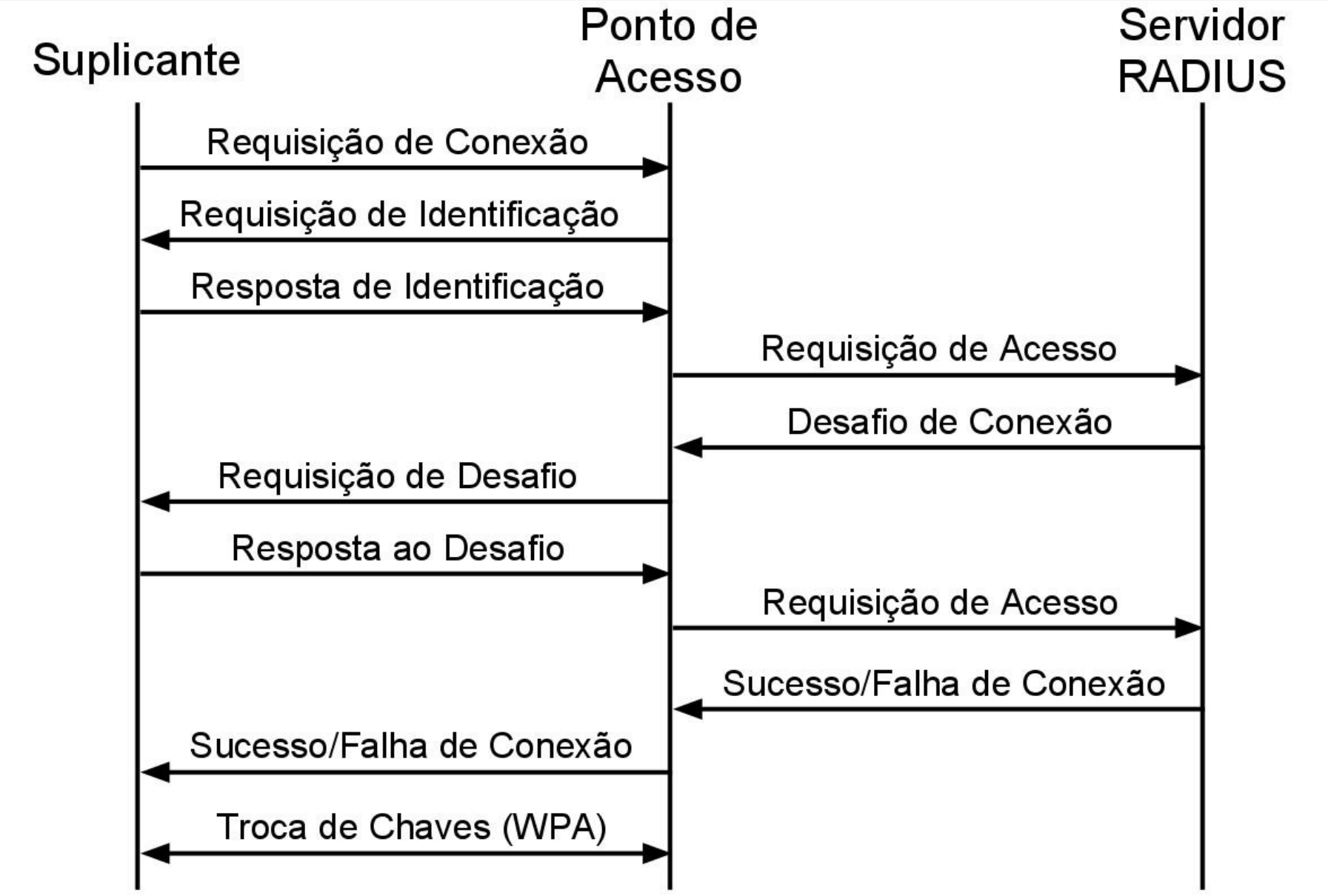
CCMP - Encriptação



Extensible Authentication Protocol

- Evolução do PPP
- Usado apenas para autenticação
- Servidor RADIUS isolado
- Muito Usado no WPA/WPA2 Comercial

EAP - Autenticação



EAP - Protocolos

- Chave Secreta: sujeito a MITM
  - EAP-MD5

- Criptografia Assimétrica
  - Meios inseguros
  - Autoridade Certificadora
  - EAP-TLS (RSA)

Conclusão

- Redes sem fio ainda inseguras
- Usuários em parte culpados
  - Chaves fracas
- Fabricantes também culpados
  - WEP continua sendo um padrão

Obrigado pela atenção

Pergunta 1

Por que é necessária a encriptação de todas as mensagens trocadas em uma rede sem fio?

Pergunta 1

Por que é necessária a encriptação de todas as mensagens trocadas em uma rede sem fio?

Porque o meio de propagação da informação é o ar e, portanto, qualquer em um certo raio de alcance terá acesso à informação que, a princípio, só um deveria ser capaz de ouvir.

Pergunta 2

Cite três maneiras de obter a chave secreta no WEP.

Pergunta 2

Cite três maneiras de obter a chave secreta no WEP.

Força Bruta com uso de dicionário, intercepção do desafio (em claro e encriptado) usado durante a conexão e escuta contínua de quadros transmitidos na rede.

Pergunta 3

Discorra sobre duas melhorias do WPA em relação ao WEP.

Pergunta 3

Discorra sobre duas melhorias do WPA em relação ao WEP.

A utilização de um novo sistema para garantir integridade das mensagens (MIC) evita ataques de troca de bits, enquanto que o uso de chaves temporais não permite que a chave compartilhada entre os participantes da rede seja utilizada diretamente para criptografia.

Pergunta 4

Quais são as duas maiores vertentes de protocolos EAP? Qual é a mais insegura?

Pergunta 4

Quais são as duas maiores vertentes de protocolos EAP? Qual é a mais insegura?

São EAP por chave secreta e EAP por criptografia assimétrica. A primeira é mais insegura por ser vulnerável a ataques de "Man-in-the-Middle".

Pergunta 5

Que precaução básica deve ser tomada a fim de evitar que chave secreta da rede sem fio seja descoberto a partir de um ataque de força bruta?

Pergunta 5

Que precaução básica deve ser tomada a fim de evitar que chave secreta da rede sem fio seja descoberto a partir de um ataque de força bruta?

O uso de chaves difíceis, que não correspondam a nenhuma palavra que possa ser descoberta a partir de um ataque de dicionário.