UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Criptografia e Certificação Digital
Terceira Aula

Prof. Frederico Sauer, D.Sc.

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Advanced Encryption Standard

- As vulnerabilidades do DES motivaram uma chamada pelo NIST por novos algoritmos

SEGURANÇA

- **Segurança real:** em comparação com outros algoritmos enviados (na mesma chave e tamanho de bloco).
- **Aleatoriedade:** até que ponto a saída do algoritmo é indistinguível de uma permutação aleatória no bloco de entrada.
- **Solidez:** da base matemática para a segurança do algoritmo.
- **Outros fatores de segurança:** levantados pelo público durante o processo de avaliação, incluindo quaisquer ataques que demonstrem que a segurança real do algoritmo é menor que a resistência afirmada por quem o enviou.

CUSTO

- **Condições de licenciamento:** O NIST pretende, quando o AES for lançado, disponibilizar o algoritmo especificado no AES ao mundo inteiro, sem exclusividade e sem royalties.
- **Eficiência computacional:** A avaliação da eficiência computacional será aplicável para implementações tanto em hardware quanto em software. A análise da primeira rodada, feita pelo NIST, focará principalmente as implementações em software e uma combinação de tamanho de chave e bloco específica (128-128); será dada mais atenção às implementações em hardware e outras combinações de tamanho de chave e bloco suportadas durante a análise da segunda rodada. A eficiência computacional basicamente refere-se à velocidade do algoritmo. Os comentários públicos sobre a eficiência de cada algoritmo (especialmente para diversas plataformas e aplicações) também será levada em consideração pelo NIST.
- **Requisitos de memória:** A memória exigida para implementar um algoritmo candidato — para implementações tanto em hardware quanto em software do algoritmo – também será considerada durante o processo de avaliação. A análise da primeira rodada pelo NIST focará principalmente as implementações em software; será dada mais atenção às implementações em hardware durante a segunda rodada. Os requisitos de memória incluirão fatores como contagens de portas para implementações em hardware e tamanho de código e requisitos de RAM para implementações em software.

ALGORITMO E CARACTERÍSTICAS DE IMPLEMENTAÇÃO

- **Flexibilidade:** Os algoritmos candidatos com maior flexibilidade atenderão às necessidades de mais usuários do que aqueles menos flexíveis e, portanto, *inter alia*, são preferíveis. Porém, alguns excessos de funcionalidade possuem pouca aplicação prática (por exemplo, tamanhos de chave extremamente curtos); para esses casos não será dada preferência. Alguns exemplos de flexibilidade podem incluir (mas não são limitados) ao seguinte:
  - **a.** O algoritmo pode aceitar tamanhos adicionais de chave e bloco (por exemplo, tamanhos de bloco de 64 bits, tamanhos de chave diferentes daqueles especificados na seção de requisitos mínimos de aceitação — por exemplo, chaves entre 128 e 256 que sejam múltiplos de 32 bits etc.).
  - **b.** O algoritmo pode ser implementado de forma segura e eficiente em uma grande variedade de plataformas e aplicações (por exemplo, processadores de 8 bits, redes ATM, comunicações por voz e satélite, HDTV, B-ISDN etc.).
  - **c.** O algoritmo pode ser implementado como uma cifra de fluxo, gerador de código de autenticação de mensagem (MAC), gerador de número pseudo-aleatório, algoritmo de hashing etc.
- **Adequação de hardware e software:** Um algoritmo candidato não deverá ser restritivo no sentido de só poder ser implementado em hardware. Se alguém também puder implementá-lo de maneira eficiente em firmware, então essa será uma vantagem na área de flexibilidade.
- **Simplicidade:** Um algoritmo candidato será julgado de acordo com a simplicidade relativa do projeto.

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

AES – Principais Requisitos

- Cifra de Bloco
- Bloco de 128 bits, chaves de 128/192/256-bits
- Mais rápido e robusto que o Triple-DES
- Vida útil estimada de 20-30 anos
- Completa especificação disponível
- Implementações em C & Java

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

AES – Escolha do Algoritmo

- Após testes e avaliações, chega-se em AGO/99:
  - MARS (IBM) - complexo, rápido, grande robustez
  - RC6 (USA) – muito simples e rápido, baixa robustez
  - Rijndael (Bélgica) – simples, rápido e robusto
  - Serpent (Euro) - lento, simples, muito robusto
  - Twofish (USA) - complexo, muito rápido e robusto
- O contraste entre os algoritmos era:
  - Poucos e complexos ciclos ou vários ciclos simples
  - Refinamento de cifras existentes ou novas propostas

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Rinjdael - Análise

Segurança geral

O Rijndael não possui ataques de segurança conhecidos. Ele usa caixas-S como componentes não lineares. O Rijndael parece ter uma margem de segurança adequada, mas recebeu críticas sugerindo que sua estrutura matemática pode conduzir a ataques. Por outro lado, a estrutura simples pode ter facilitado sua análise de segurança durante o período de tempo do processo de desenvolvimento do AES.

Implementações em software

O Rijndael realiza criptografia e decriptografia muito bem em diversas plataformas, incluindo as de 8 bits e 64 bits, e DSPs. Porém, existe uma queda no desempenho com tamanhos de chave maiores, em razão do número maior de rodadas executadas. O alto paralelismo inerente ao Rijndael facilita o uso eficiente dos recursos do processador, resultando um desempenho de software muito bom, mesmo quando implementado em um modo sem capacidade de intercalação. O tempo de configuração de chaves do Rijndael é pequeno.

Ambientes de espaço restrito

Em geral, o Rijndael é muito bem adequado a ambientes de espaço restrito, nos quais a criptografia ou decriptografia (mas não ambas) são implementadas. Ele possui requisitos muito baixos de RAM e ROM. Uma desvantagem é que os requisitos de ROM aumentarão se a criptografia e a decriptografia forem implementadas simultaneamente, embora pareça continuar adequado a esses ambientes. O escalonamento de chaves para decriptografia é separado da criptografia.

Implementações em hardware

O Rijndael possui o throughput mais alto que qualquer um dos finalistas para os modos com feedback e o segundo mais alto para os modos sem feedback. Para os tamanhos de chave de 192 e 256 bits, o throughput cai nas implementações padrão e desdobrada, devido ao número adicional de rodadas. Para implementações totalmente em pipeline, o requisito de área aumenta, mas o throughput não é afetado.

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Rinjdael - Análise

Ataques nas implementações

As operações usadas pelo Rijndael estão entre as mais fáceis de serem defendidas contra ataques de consumo de potência e temporização. O uso de técnicas de máscara para defender o Rijndael contra esses ataques não causa degradação significativa no desempenho em comparação aos outros finalistas, e seu requisito de RAM continua sendo razoável. O Rijndael parece obter uma vantagem de velocidade importante em relação aos seus concorrentes quando essas proteções são consideradas.

Criptografia *versus* decriptografia

As funções de criptografia e decriptografia no Rijndael são diferentes. Um estudo do FPGA relata que a implementação conjunta de criptografia e decriptografia ocupa cerca de sessenta por cento mais espaço do que a implementação isolada da criptografia. A velocidade do Rijndael não varia significativamente entre a criptografia e a decriptografia, embora o desempenho da configuração das chaves na decriptografia seja mais lento do que na criptografia.

Agilidade da chave

O Rijndael admite cálculo de subchave sob demanda para a criptografia. Ele requer uma única execução do escalonamento de chaves para gerar todas as subchaves antes da primeira decriptografia com uma chave específica. Isso exige um pouco mais de recursos para a agilidade da chave do Rijndael.

Outras versatilidades e flexibilidades

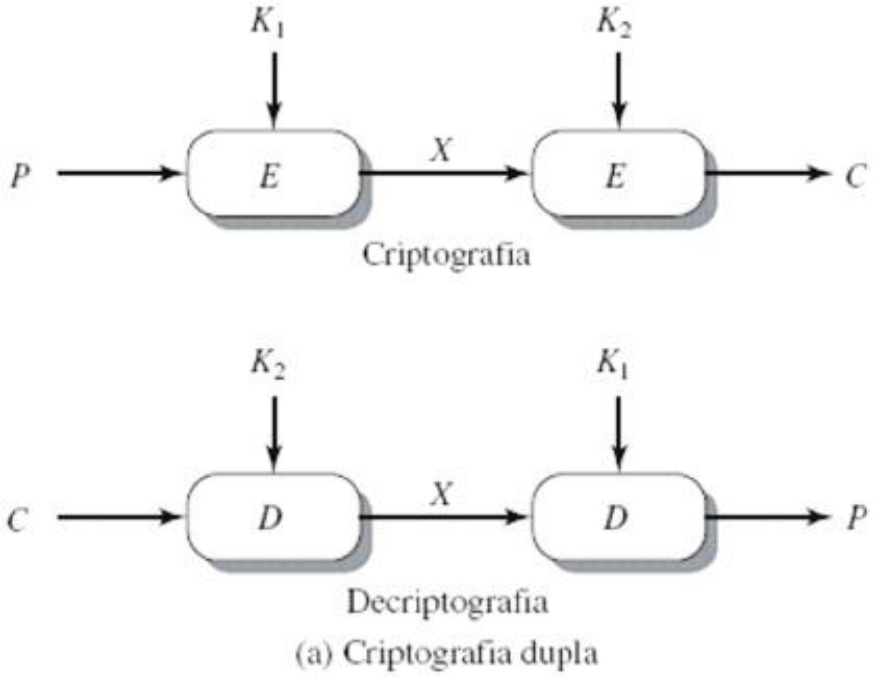
O Rijndael admite qualquer combinação de tamanhos de bloco e de chave de 128 bits, 192 bits e 256 bits. A princípio, a estrutura do Rijndael pode acomodar quaisquer tamanhos de bloco e combinações de chave que sejam múltiplos de 32, além de mudanças no número de rodadas especificadas.

Potencial para paralelismo em nível de instrução

O Rijndael possui um excelente potencial para paralelismo em uma criptografia de bloco único.

Múltiplas Encriptações

- Uma solução para as fragilidades do DES é a múltipla criptografia



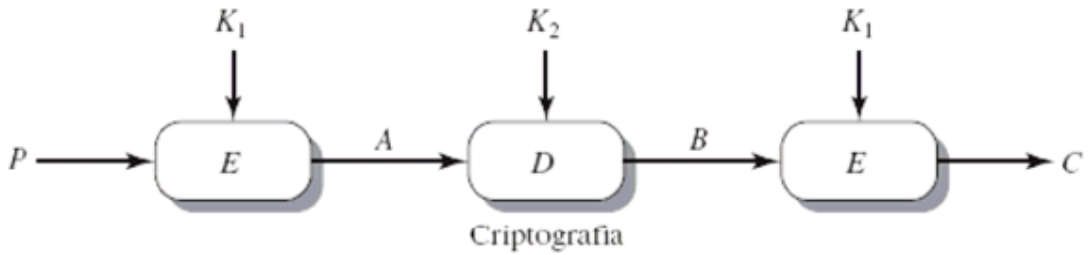
(a) Criptografia dupla

Permite ataque por bruta força.
Como $X = E_{K1}(P) = D_{K2}(C)$, usando todas chaves possíveis para encriptar P e após isso fazer o mesmo decriptando C até combinar o valor de X.

O ataque é da ordem de 2^{56}

3-DES

- Uma solução é o uso de 3 cifragens com 2 chaves distintas na forma $C = E_{K1}(D_{K2}(E_{K1}(P)))$



(b) Criptografia tripla

3-DES

- Pode ser ainda usado com 3 chaves na forma $C = E_{K3}(D_{K2}(E_{K1}(P)))$
- Disponível em algumas aplicações da Internet, como o pgp e o S-MIME

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Modos de Operação

- As cifras de bloco operam com blocos de dados de tamanhos fixos (DES – 64 bits)
- Os modos de operação permitem que o AES e o DES cifrem/decifrem quantidades arbitrárias de dados

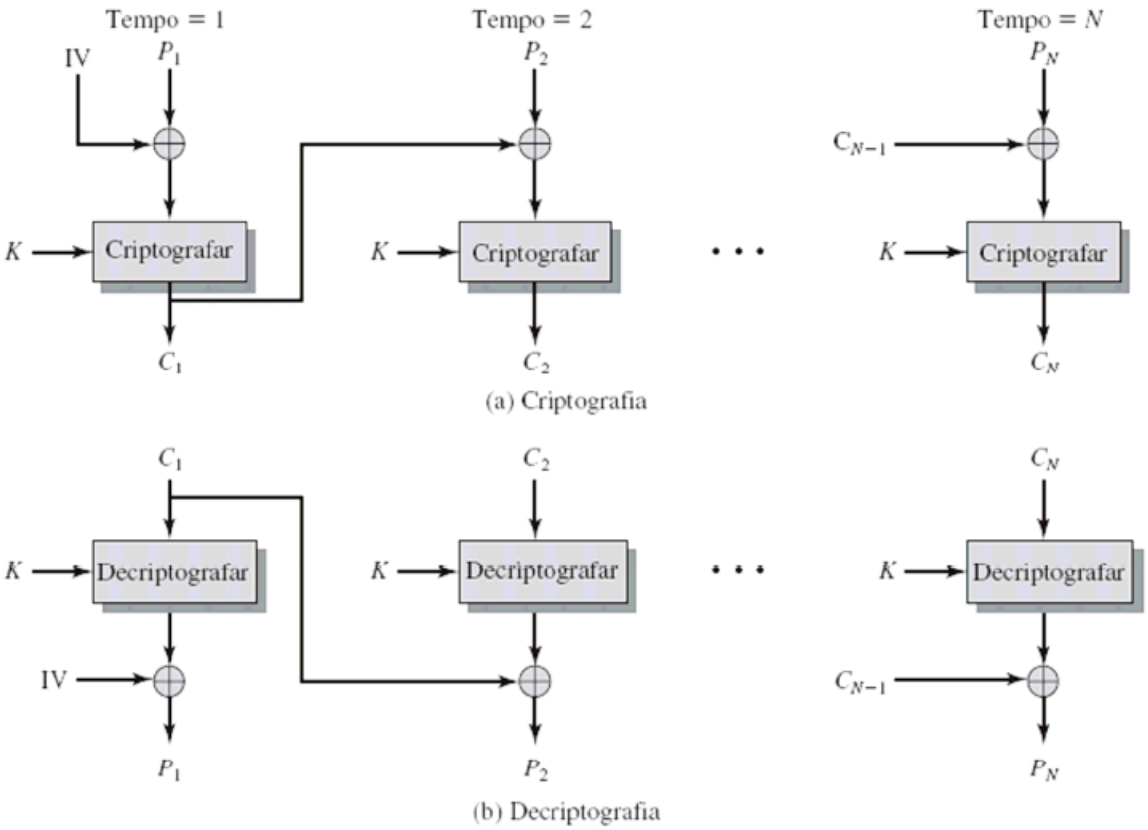
UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Modos de Operação

Modo	Descrição	Aplicação típica
Electronic Codebook (ECB)	Cada bloco de 64 bits de texto claro é codificado independentemente, usando-se a mesma chave.	• Transmissão segura de valores isolados (por exemplo, uma chave criptográfica)
Cipher Block Chaining (CBC)	A entrada do algoritmo criptográfico é o XOR dos próximos 64 bits de texto claro e os 64 bits anteriores de texto crifrado.	• Transmissão de uso geral orientada a bloco • Autenticação
Cipher Feedback (CFB)	A entrada é processada *j* bits de cada vez. O texto crifrado anterior é usado como entrada para o algoritmo criptográfico de forma a produzir uma saída pseudo-aleatória, que é XORada com o texto claro para produzir a próxima unidade de texto cifrado.	• Transmissão de uso geral orientada a fluxo • Autenticação
Output Feedback (OFB)	Semelhante ao CFB, exceto que a entrada do algoritmo criptográfico é a saída DES anterior.	• Transmissão orientada a fluxo por canal com ruído (por exemplo, comunicação por satélite)
Counter (CTR)	Cada bloco de texto claro é XORado com um contador criptografado. O contador é incrementado para cada bloco subseqüente.	• Transmissão orientada a bloco de uso geral • Útil para requisitos de alta velocidade

Um exemplo - CBC

- Útil para grandes volumes de dados
- Cria uma cadeia de dependência entre os dados (propaga erro)
- Usa um segredo a mais: IV

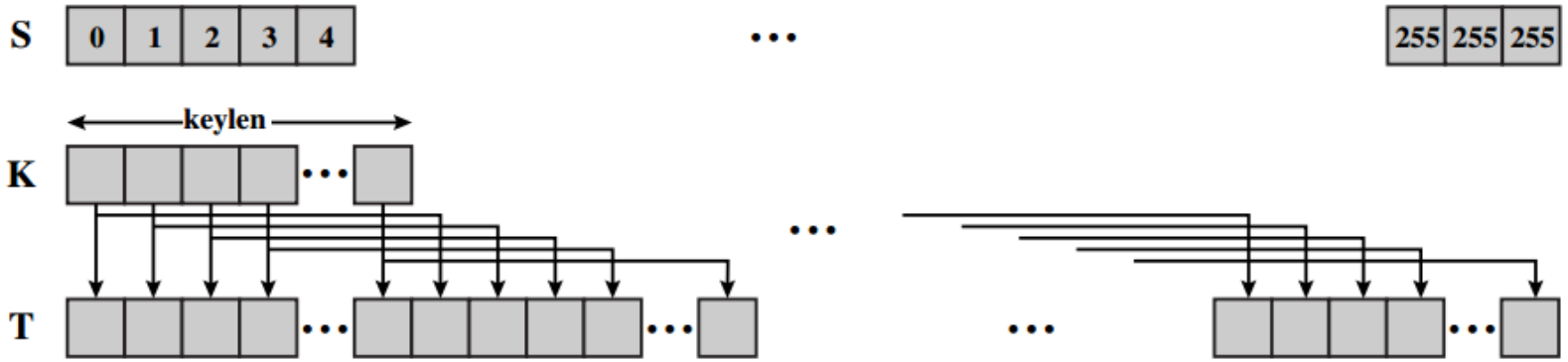


RC4

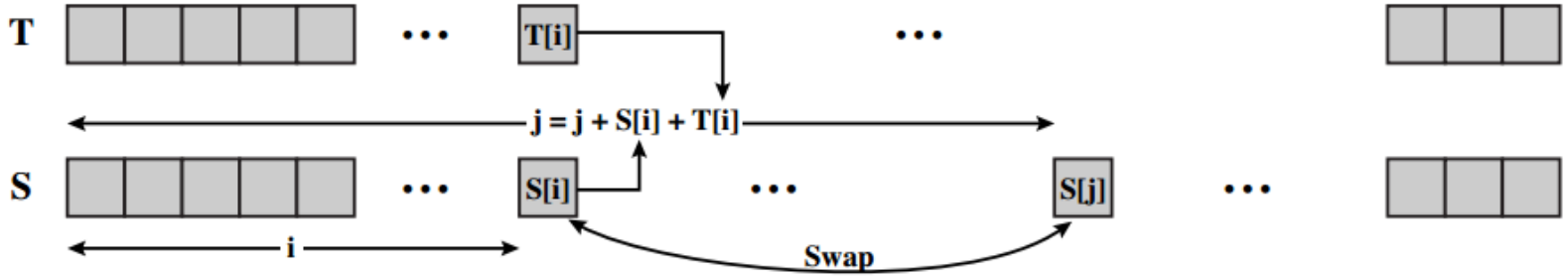
- Algoritmo da RSA
- Simples e rápido, porém robusto
- Cifra de fluxo orientada a byte
- Tamanho variável de chave, que é permutada randomicamente
- Usado pelo web SSL/TLS e WEP

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

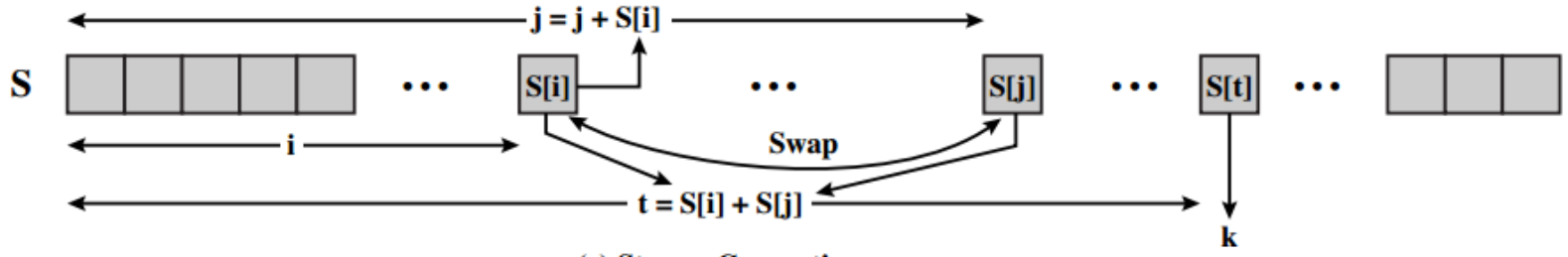
Operação do RC4



(a) Initial state of S and T



(b) Initial permutation of S



(c) Stream Generation

Aspectos da Criptografia Simétrica

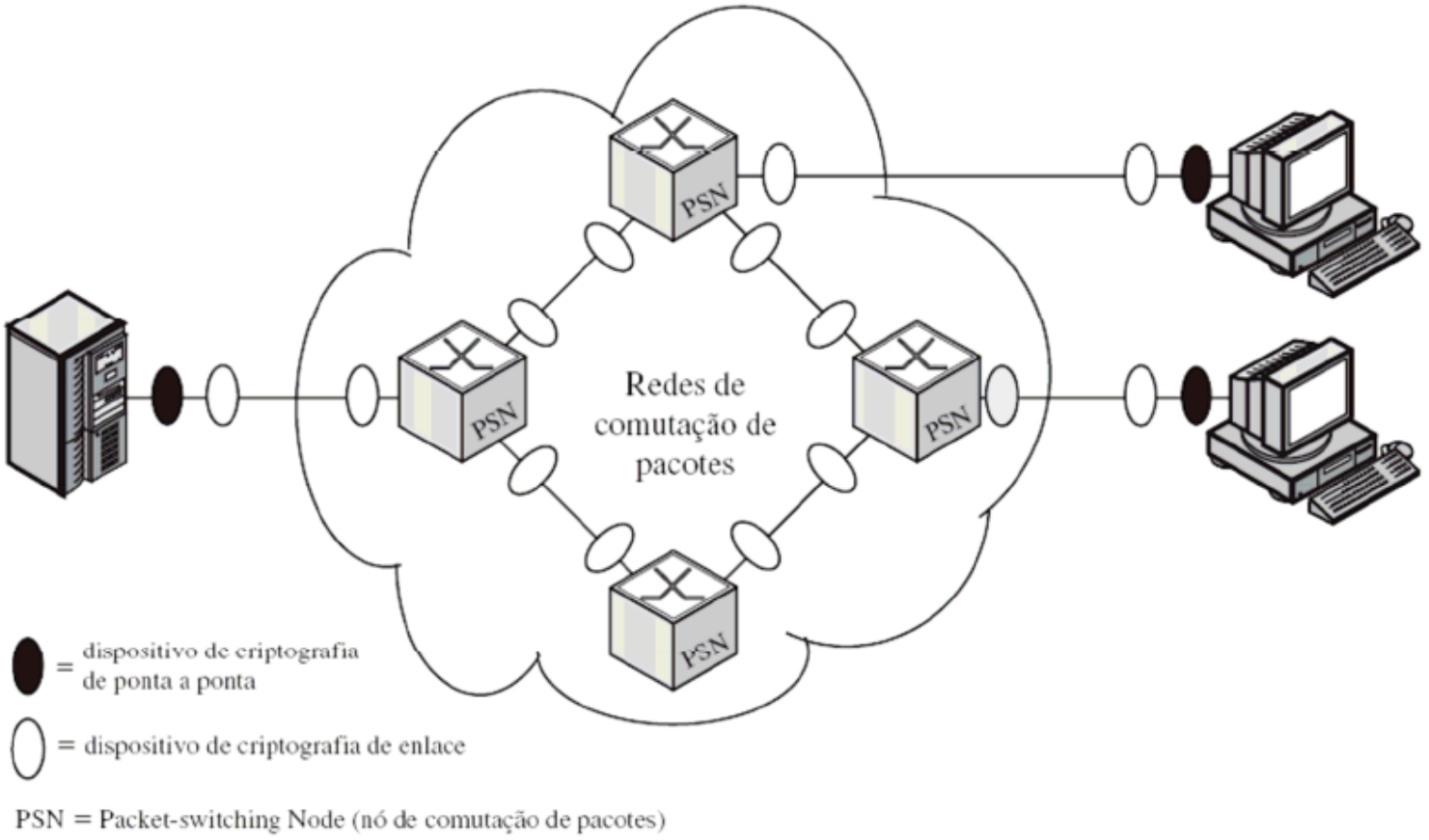
- Algoritmos simétricos são rápidos e passíveis de implementação em hardware
- Sua robustez depende diretamente da manipulação adequada da chave (ex. WEP)

Tabela 6.2 Comparação das velocidades das cifras simétricas em um Pentium II.

Cifra	Tamanho de chave	Velocidade (Mbps)
DES	56	9
3DES	168	3
RC2	variável	0,9
RC4	variável	45

Confidencialidade com Criptografia Simétrica

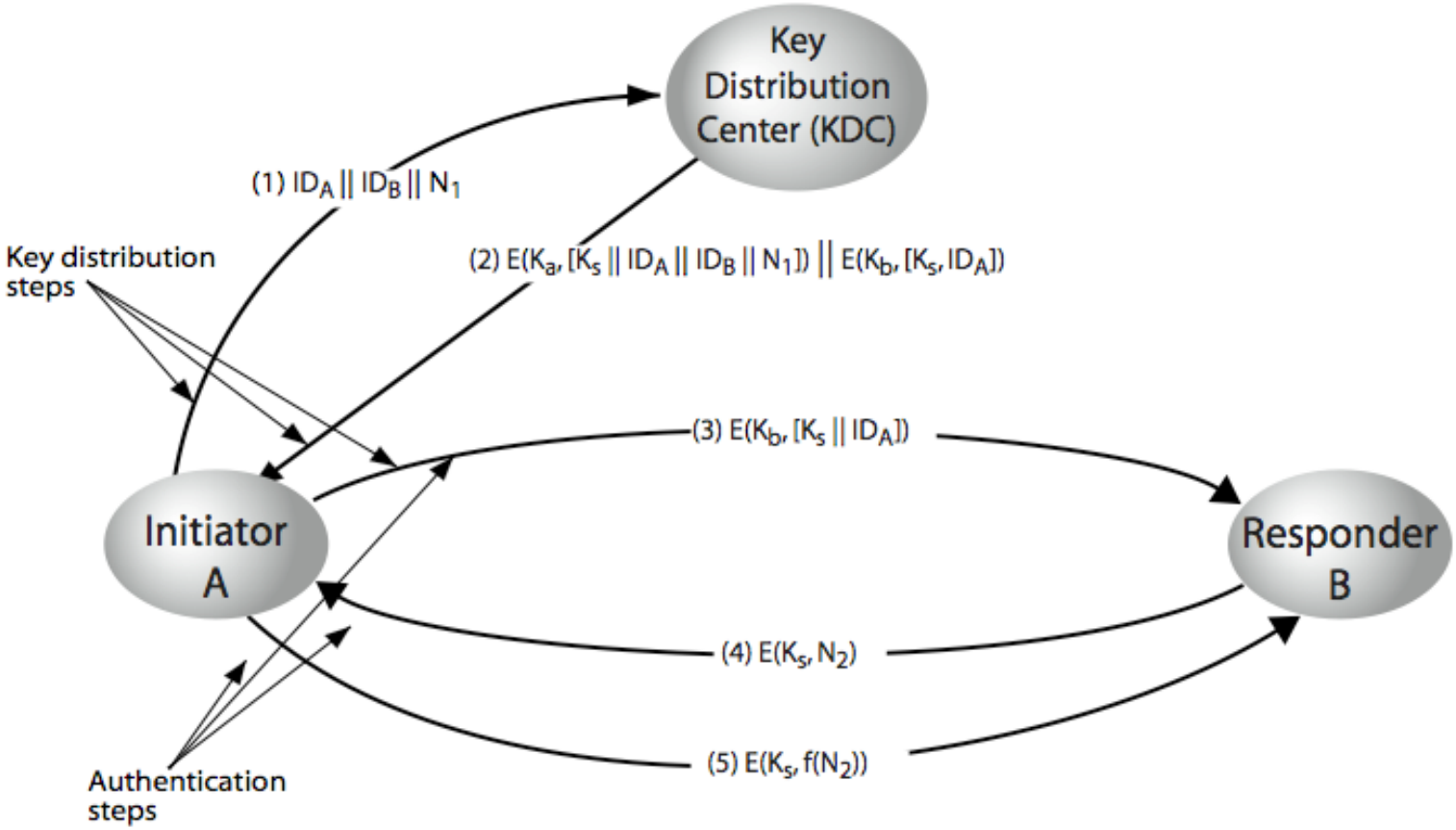
- Alternativas de implementação:



UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Drawbacks das Opções

Criptografia de enlace	Criptografia de ponta a ponta
Segurança dentro dos sistemas finais e sistemas intermediários	
Mensagem exposta no host emissor	Mensagem criptografada no host emissor
Mensagem exposta nos nós intermediários	Mensagem criptografada nos nós intermediários
Papel do usuário	
Aplicado pelo host emissor	Aplicado pelo processo emissor
Transparente ao usuário	Usuário aplica criptografia
Host mantém recurso de criptografia	Usuário precisa determinar algoritmo
Um recurso para todos os usuários	Usuários selecionam esquema de criptografia
Pode ser feito no hardware	Implementação de software
Todas ou nenhuma mensagem criptografada	Usuário escolhe criptografar ou não, para cada mensagem
Problemas de implementação	
Exige uma chave por par (host/nó intermediário) e par (nó intermediário/ nó intermediário)	Exige uma chave por par de usuários
Oferece autenticação de host	Oferece autenticação do usuário

Distribuição de Chaves

- Tipos de Chaves
  - Session Key (K_s)
  - Master Key (K_a, K_b)