Criptografia/Criptografia Aplicada 2020/2021 – Época Normal – 18 Janeiro de 2021

Duração: 2h

Número mecanográfico: | | | | | | | | | |

Nome completo: _____

Grupo 1 - Segurança Criptográfica e Aleatoriedade *(15%)*

1.1. One Time Pad.

O One-Time-Pad é seguro num modelo de ataque em que o adversário pode ter as seguintes capacidades [ ]

[pode ser computacionalmente ilimitado desde que observe apenas um criptograma criado com cada chave]

As duas limitações principais práticas do One-Time-Pad são [ ]

[chaves do tamanho das mensagens, chaves simétricas pré-partilhadas que só podem ser utilizadas uma vez].

1.2. Distribuições Simples.

Seja $p > 2$ um inteiro primo, e $\ell > 0, \lambda \geq \ell$ inteiros. Seja $x \leftarrow_\$ [k]$ a operação de amostrar um valor com a distribuição uniforme do conjunto de inteiros $\{0, \ldots, k-1\}$. As seguintes distribuições são uniformes?

Distribuição	Sim	Não
$\{ x \mod p \mid x \leftarrow_\$ [2^\lambda] \}$		x
$\{ x \mod p \mid x \leftarrow_\$ [2^\lambda \cdot p] \}$	x	
$\{ x \mod p \mid x \leftarrow_\$ [2^{\lambda+p}] \}$		x
$\{ x \mod 2^\ell \mid x \leftarrow_\$ [p] \}$		x
$\{ x \mod 2^\ell \mid x \leftarrow_\$ [2^\lambda + p] \}$		x

Distribuição	Sim	Não
$\{ x \mod p \mid x \leftarrow_\$ [p] \}$	x	
$\{ x \mod p \mid x \leftarrow_\$ [2^\lambda + p] \}$		x
$\{ x \mod 2^\ell \mid x \leftarrow_\$ [2^\lambda] \}$	x	
$\{ x \mod 2^\ell \mid x \leftarrow_\$ [2^\lambda \cdot p] \}$	x	
$\{ x \mod 2^\ell \mid x \leftarrow_\$ [2^{\lambda+p}] \}$	x	

1.3. Pseudo-Aleatoriedade

Um processo que consome λ bits de aleatoriedade e produz outputs de tamanho 2λ (pode/não pode) [não pode] produzir distribuições uniformes sobre o seu contradomínio.

Um processo que consome 2λ bits de aleatoriedade e produz outputs de tamanho λ (pode/não pode) [pode] produzir distribuições uniformes sobre o seu contradomínio.

Um algoritmo (probabilístico/determinístico) [deterministico] que consome λ bits de aleatoriedade é um gerador pseudo-aleatório se [o output produzido for indistinguível de uma string uniforme].

Um gerador pseudo-aleatório recebe como input uma sequência de bits, conhecida como [seed/semente], amostrada de uma distribuição [uniforme].

1.4. Segurança Heurística e Demonstrável

De que forma é justificada a segurança das seguintes primitivas/construções criptográficas.

Construção/primitiva	**Demonstrável**	**Heurística**
Counter-Mode	x	
Davis-Meyer	x	
Função RSA		x
Problema Diffie-Hellman		x
Merkle-Damgard	x	
AES		x

1.5. Desenvolvimento. *(5%)*

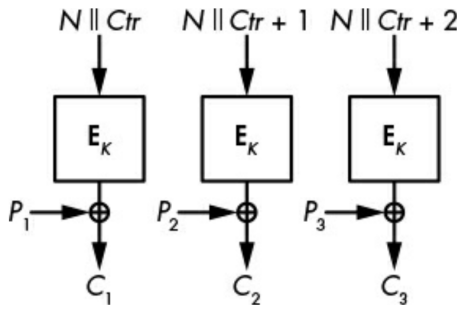
Explique os conceitos de segurança perfeita e ataque por força bruta. Discuta de que forma se aplicam estes conceitos ao One Time Pad.

Num. Mec. | | | | | | | | | | Nome:

Grupo 2 - Criptografia Simétrica *(30%)*

2.1. Aplicações do AES.

a) Considere o seguinte diagrama



O diagrama descreve o esquema [counter-mode] que se classifica como uma construção de [cifra simétrica].

Utiliza E_k como um componente que geralmente é instanciado com uma construção de [cifra de blocos].

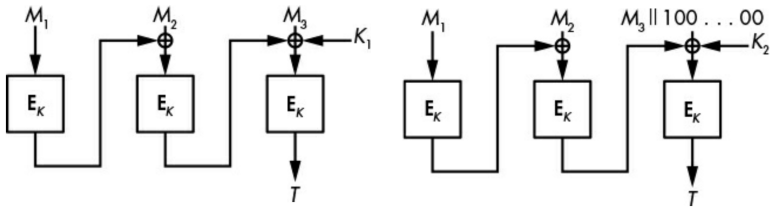
O Advanced Encryption Standard (AES), para um nível de segurança de 128-bits, utiliza chaves de tamanho [128 bits], aceita inputs de tamanho [128 bits] e produz outputs de tamanho [128 bits].

Um nível estimado de segurança de 128-bits significa que [o melhor ataque conhecido precisa de realizar 2^128 operações/passos computacionais].

O esquema no diagrama permite garantir [confidencialidade], uma propriedade que é formalizada pela noção de [criptogramas] [indistinguiveis] contra atacantes [(com acesso a) texto-limpos escolhidos], usualmente designada pela sigla [IND-CPA].

O esquema será seguro quando utilizado com o AES se o AES cumprir o pressuposto de [PRF/PRP].

b) Considere os seguintes diagramas, em que do lado esquerdo M_3 é do tamanho do input de E_k e do lado direito isto não acontece.



Os diagramas descrevem o esquema [CMAC] que se classifica como uma construção de [Message Authentication Code /MAC].

O esquema no diagrama permite garantir [autenticidade/ integridade], uma propriedade que é formalizada pela noção de [dificuldade] [em falsificar/unforgeability] contra atacantes [(com acesso a) texto-limpos/msg escolhidas], usualmente designada pela sigla [UF-CMA].

Este esquema não protege contra ataques [de repetição/reordenamento de mensagens], a nao ser que se garanta que cada mensagem só é transmitida uma vez.

A construção [E.g., HMAC ou Wegman Carter] oferece as mesmas garantias mas é mais eficiente, porque utiliza [funções de hash / hashing universal] como componente(s) principal(ais).

2.2. Cifras Simétricas

O RC4 é uma construção de cifra sequencial cuja utilização atualmente é insegura/não recomendada.

O núcleo do RC4 é uma construção de PRG/gerador pseudo-aleatório em que a chave da cifra é utilizada como semente.

Como em todas as cifras deste tipo, o núcleo tem de ser determinístico porque na operação de decifração a decifração tem de gerar o mesmo stream de chaves.

2.3. Merkle Damgård

A construção Merkle Damgård transforma uma função de compressão numa função de hash.

Em termos da sua segurança, a construção de Merkle Damgård é resistente a colisões se o seu sub-componente for resistente a colisões.

A construção de Davis-Mayer transforma uma cifra de blocos numa função de compressão, e relaciona-se com a construção de Merkle Damgård porque pode instanciar o seu componente fundamental.

2.4. Funções de Hash

Uma função de hash com tamanho de output λ é vulnerável a um ataque que encontra uma colisão em aproximadamente 2^(lambda/2) passos e que usualmente se chama birthday attack ou ataque do aniversário.

Por este motivo, quando se pretende um nível de segurança de λ bits, o tamanho do output das funções de hash utilizadas é geralmente 2 * lambda.

A construção Poly-1305 tem um output com tamanho 128 bits (o número de bits de segurança mais usado hoje em dia) e não é vulnerável ao ataque anterior porque é uma construção de MAC, na qual não é possível procurar por colisões sem saber a chave

2.5. Desenvolvimento. *(10%)*

Explique a construção de Wegman-Carter e discuta até que ponto poderá ser uma função pseudo-aleatória.

Num. Mec. | | | | | | | | | | Nome:

Grupo 3 - Criptografia Assimétrica *(25%)*

3.1. Aplicações do RSA.

a) O problema RSA diz que, para parâmetros públicos (n, e) e função $RSA(x) := x^e \mod n$ é difícil

inverter a função (encontrar x) se x for escolhido de forma aleatória .

b) O valor $y = RSA(m)$ não garante confidencialidade de m porque

é determinístico e, portanto, inseguro no modelo IND-CPA .

c) O problema RSA é o pressuposto computacional subjacente ao esquema RSA-OAEP que garante confidencialidade de acordo com o modelo IND-CPA/IND-CCA .

3.2. Aplicações do Diffie-Hellman.

a) O problema computacional Diffie-Hellman diz que, para num grupo G de tamanho primo q, gerador g e operação de grupo $\circ$ é difícil dados g^x e g^y para x, y aleatórios, encontrar g^(xy)

.

b) O problema computacional Diffie-Hellman é o pressuposto computacional subjacente ao esquema ElGamal que garante confidencialidade de acordo com o modelo IND-CPA .

3.3. Problemas computacionais.

a) Atribua (1) ou (2) aos problemas em cada uma das linhas seguintes, para que façam sentido na frase:

Se existir um algoritmo que resolve de forma eficiente o problema (1), então existe um algoritmo que resolve de forma eficiente o problema (2).

Diffie-Hellman Computational	2	Logaritmo Discreto	1
Factorização de Inteiros	1	Problema RSA	2
Encontrar Colisões em H	2	Encontrar pré-imagens em H	1

b) Nas perguntas anteriores os problemas (1) são potencialmente mais (fáceis/difíceis) difíceis de resolver que os problemas (2).

3.4. Cifras Assimétricas.

Uma cifra assimétrica permite ao emissor enviar informação com garantias de confidencialidade ao recetor necessitando para isso de garantias de autenticidade sobre a chave pública do recetor.

As cifras assimétricas utilizam geralmente o paradigma KEM/DEM, e são portanto técnicas híbridas porque

combinam técnicas simétricas e assimétricas .

3.5. Assinaturas Digitais.

a) Uma assinatura digital deve garantir autenticidade, integridade e não repúdio

mas não garante confidencialidade.

O algoritmo de verificação de uma assinatura digital recebe como inputs mensagem, assinatura e chave pública

e retorna um bit/boleano a indicar validade/invalidade.

b) A assinatura de Schnorr consiste num par (r, s), em que $r = g^k$ e $s = k - x \cdot H(r||M)$. Explique porque é que a repetição da aleatoriedade r permite um ataque a este esquema.

3.6. Desenvolvimento. *(10%)*

A assinatura digital RSA Full Domain Hash calcula $\sigma = H(m)^d \mod n$. Explique como funciona o processo de verificação da assinatura e porque é que a propriedade da unidirecionalidade da função RSA poderá não ser suficiente para garantir a segurança da construção.

Num. Mec. | | | | | | | | | | Nome:

Grupo 4 - Protocolos e PKI *(30%)*

4.1. Cifras Autenticadas

a) A cifra autenticada Encrypt-And-MAC é [insegura] (segura/insegura) no modelo IND-CPA se for implementada com base numa cifra IND-CPA segura e um MAC que é uma PRF.

A cifra autenticada Encrypt-Then-MAC é [segura] (segura/insegura) no modelo IND-CPA se for implementada com base numa cifra IND-CPA segura e um MAC que é uma PRF.

Se escreveu **insegura** em uma ou nas duas frases acima, justifique:

[ ]

Uma cifra autenticada garante as propriedades de segurança [confidencialidade, autenticidade, integridade].

b) A primitiva AEAD é diferente de uma cifra autenticada porque [permite autenticar metadados juntamente com o criptograma]

[ ]

A primitiva AEAD foi adotada como a abstração correta em protocolos como TLS porque [ ]

[a autenticação de metadados permite autenticar o header/números de sequência e oferece as garantias de segurança necessárias num canal seguro]

As duas construções de AEAD recomendadas pela versão 1.3 do TLS são [ ]

[AES-GCM, ChaCha20-Poly1305].

4.2. Gestão de Chaves

Num cenário com N utilizadores que pretendem comunicar utilizando criptografia simétrica com garantias de segurança ponto a ponto (i.e., entre cada par de utilizadores):

a) se utilizarmos apenas pré-distribuição de chaves de longa duração, no mínimo, cada utilizador necessita de armazenar [N-1] chaves de forma permanente, e globalmente teremos de gerir [N*(N-1)/2] chaves de longa duração.

b) se utilizarmos um agente de confiança para distribuição de chaves de sessão, cada utilizador necessita de armazenar [1] chaves de forma permanente, e globalmente teremos de gerir [N] chaves de longa duração.

c) O que muda relativamente à alínea b) se considerarmos a utilização de criptografia assimétrica?

[ ]

4.3. Certificados de Chave Pública

Os certificados de chave pública podem ser transferidos por canais inseguros desde que

desde que não sejam de raiz/desde que possam ser validados utilizando outros certificados.

Um certificado de raiz pode ser facilmente reconhecido porque

é assinado pelo titular/auto-assinado/o issuer e o subject são o mesmo.

A assinatura digital num certificado de raiz não é relevante para a sua segurança porque

a confiança é estabelecida por um canal não criptográfico e o certificado não é validado com base na assinatura (confiança implícita).

(**Bónus**) Dê um exemplo de uma assinatura insegura, mas que seja utilizada na prática exatamente no contexto anterior

assinaturas com base em SHA-1.

4.4. Desenvolvimento. *(10%)*

Suponha que dois agentes A e B estabelecem uma chave criptográfica utilizando o protocolo Diffie-Hellman autenticado (e.g., Station-to-Station).

A e B utilizam chaves públicas certificadas pelas Autoridades de Certificação CA_A e CA_B, respectivamente, ambas subordinadas da mesma CA Root em quem A e B confiam implicitamente.

Suponha que um atacante obtém a chave privada de CA Root. Discuta em que circunstâncias poderia quebrar:

a) uma sessão estabelecida no passado (antes da corrupção da chave de CA Root) e

b) uma sessão a estabelecer no futuro.