

Número mecanográfico:

Versão A

Nome completo: _____

Grupo 1 - Segurança Criptográfica e Aleatoriedade (20%)

1.1. One Time Pad.

Suponha que o One-Time-Pad é utilizado para proteger as comunicações entre dois pontos A e B , que poderão implicar a transmissão de até 1GByte de informação em cada sentido, por dia.

Tendo em conta que não pode utilizar nenhuma outra técnica criptográfica, responda às seguintes questões.

- Explique a gestão e operação deste sistema para garantir confidencialidade das comunicações para o caso em que o canal de comunicação não pode ser perturbado por um atacante.

- Discuta até que ponto este sistema pode garantir segurança da informação (confidencialidade, integridade, autenticidade) no caso em que um atacante pode modificar, apagar ou inserir mensagens no canal.

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 $\{0, \dots, k-1\}$. As seguintes distribuições são uniformes?

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

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

1.3. Pseudo-Aleatoriedade

1. Explique o que entende por um gerador pseudo-aleatório que recebe m bits e produz n bits, em que $n > m$

Algoritmo que segue uma distribuição aleatória não uniforme, dado que produz uma sequencia de bits superior ao tamanho de input

2. Explique porque é que não é possível que um gerador pseudo-aleatório como o que descreveu em cima produza bit-strings de tamanho n com a distribuição uniforme.

Para um gerador pseudo-aleatório seguir uma distribuição uniforme aleatória era necessário que o tamanho do output fosse igual ou múltiplo do mesmo, caso contrário não se realiza a uniformidade

1.4. Dificuldade Computacional

Um ataque por força bruta a uma primitiva criptográfica que utiliza chaves com λ bits implica **2^{λ}**

passos computacionais, porque este ataque consiste em **explorar todas as soluções possíveis**

Uma primitiva criptográfica garante λ -bits de segurança se **o tamanho do output for 2λ -bits**

"Se o melhor ataque que se conhece contra uma primitiva criptográfica é exponencialmente mais rápido do que enumerar todas as chaves possíveis, então essa primitiva é insegura." Esta afirmação é verdadeira? Justifique.

Não de todo, pois basta que o número de bits seja suficientemente grande para que o cálculo do melhor ataque demore mais tempo do que o tempo útil, para a primitiva ser segura no sentido do melhor ataque

1.5. Segurança Heurística.

Explique os conceitos de segurança heurística e segurança demonstrável, dando exemplos de construções criptográficas que sejam validades de acordo com cada uma destas metodologias.

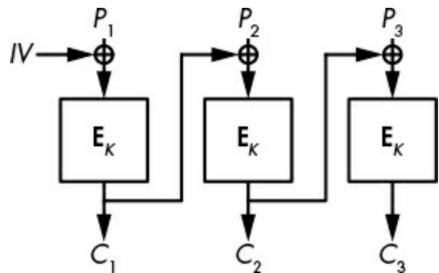
Segurança heurística consiste na realização de competições/fundações, cujo o objetivo é descrever uma nova especificação de uma construção criptográfica. Para tal, as equipas participadoras de criptógrafos e criptoanalistas, descrevem o design da sua construção e uma vez descritas, avaliam as construções das outras equipas, criticando e descobrindo falhas que possam existir nestas, de modo a que no final se chegue a uma construção que seja a mais segura na opinião da comunidade.

Um exemplo de uma construção descrita através destas competições é o SHA-3.

Segurança demonstrável incide na formalização de provas matemáticas que verificam a construção, tendo o problema que é necessitarem de resolver um problema hard matemático para que a prova seja considerada como verdadeira.

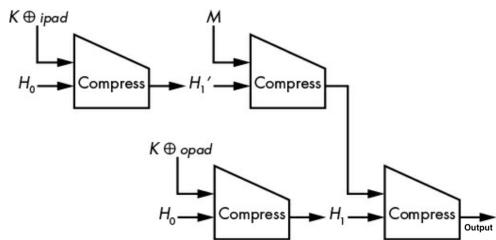
Grupo 2 - Criptografia Simétrica (20%)**2.1. Aplicações de difras de bloco.**

- a) Identifique o esquema na figura, explique as propriedades de segurança que permite garantir quando utilizado corretamente (explique o que uma utilização correta significa).



A presente construção especifica uma cifra de bloco no modo de operação CBC (Cipher Based). Tem duas vantagens graças ao seu vetor de inicialização IV: como este valor é aleatório permite-nos obter com grande probabilidade que os outputs vão ser sempre diferentes dos inputs. Também devido a esta vetor de inicialização é garantido o IND-CPA, dado que com vetores de inicalização diferentes, os outputs para o mesmo input são sempre diferentes.

- b) Considere o seguinte diagrama. Identifique o esquema na figura, explique as propriedades de segurança que permite garantir quando utilizado corretamente (explique o que uma utilização correta significa).



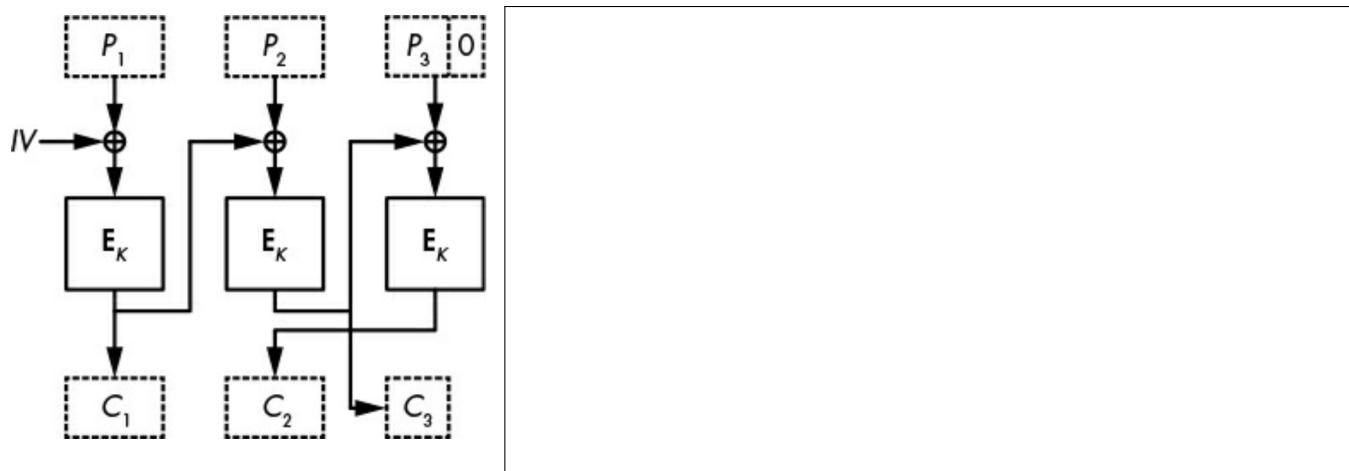
O diagrama ao lado representa a construção do HMAC, uma função de hash que cumpre o modelo de segurança UF-CMA. Esta construção conjuga a construção de Merkle-Damgard

- c) O AES pode ser utilizado como um componente em cada uma das construções anteriores? Justifique a sua resposta para cada caso.

Pode apenas ser utilizado com a cifra de bloco CBC, dado que o AES é uma construção de cifra simétrica. Como o HMAC é uma construção de Keyed Hashing não pode conjugar o AES.

2.2.

Considere o esquema no diagrama. Explique como funciona e a qual a relação com a construção da alínea a) da pergunta anterior.

**2.3. Modelos de Segurança.**

Explique os modelos de segurança IND-CPA e UF-CMA e esclareça as propriedades de segurança que representam. A qual/quais dos esquemas anteriores se aplicam?

O modelo de segurança IND-CPA garante que a confidencialidade da construção é garantida, ao qual o UF-CMA garante que a integridade da construção é garantida. Nos esquemas anteriores o IND-CPA aplica-se à cifra de bloco CBC e UF-CMA ao HMAC.

Grupo 3 - Funções de Hash (20%)

3.1. Merkle Damgård

- a) Dê um exemplo de uma função de hash que utilize a construção de Merkle-Damgård e de uma outra que não utilize esta construção.

Utiliza: MD5, Não Utiliza: SHA-3

- b) Dê um exemplo de uma propriedade indesejável da construção de Merkle-Damgård, conjuntamente com uma aplicação prática de funções de hash onde essa propriedade possa causar problemas de segurança.

Text

3.2. Funções de Hash

- a) Descreva um algoritmo que demonstre que nenhuma função de hash com tamanho de output λ pode oferecer resistência a colisões superior a $\lambda/2$ bits de segurança.

Birthday attack

- b) É possível encontrar uma aplicação em que a resistência a colisões de uma função de hash é determinante para a segurança do sistema, mas em que a dificuldade de inverter a função de hash não seja um problema?

Grupo 4 - Criptografia Assimétrica (20%)

4.1. Aplicações do RSA.

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

- a) Apresente um atacante que quebra a cifra $c = RSA(m)$, para mensagem m e criptograma c , no modelo IND-CPA.

Dado que o RSA é determinístico, ou seja para a mesma mensagem obtemos cífras iguais, então o modelo IND-CPA não é cumprido, porque para a mesma mensagem as cífras não são indistinguíveis. Isto significa que para quebrar o RSA neste modelo, basta passar-lhe mensagens diferentes e comparar o output, encontrar semelhanças.

- b) O atacante que descreveu implica que a função RSA é fácil de inverter? Justifique a sua resposta.

Não, para inverter a função RSA é necessário obter os valores dos parâmetros privados (n, d) , que podem ser calculados através do valor e , que é desconhecido.

4.2. Aplicações do Diffie-Hellman e Logaritmo Discreto.

O esquema criptográfico ElGamal define uma chave pública como $pk = g^x$, sendo a chave privada x . Dada uma mensagem m , calcula $(g^r, m \oplus H(pk^r))$

- a) O ElGamal é um protocolo de acordo de chaves, uma assinatura digital ou uma cifra assimétrica? Que tipo de garantia de segurança é oferecido por este esquema?

O ElGamal é um esquema criptográfico de cifra assimétrica, que garante a confidencialidade, autenticidade, integridade e não repúdio na cifração de mensagens.

- b) Discuta se/como um atacante consegue quebrar a segurança IND-CPA deste esquema se souber resolver o problema do logaritmo discreto.

O problema do logaritmo discreto descreve que é difícil encontrar um valor “ x ”, tal que para dois valores superiores a zero, “ a ” e “ b ”, e um número positivo “ p ”, $a^x \equiv (congruente) b \text{ mod } (p)$. Se o atacante conseguir resolver este problema, então consegue determinar o valor x , que representa a chave privada no esquema ElGamal, podendo assim inverter a cifra e obter a mensagem original.

4.3. 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

1

Diffie-Hellman Decisão

2

Problema RSA

2

Factorização de Inteiros

1

Encontrar pré-imagem em H

1

Encontrar segunda pré-imagem em H

2

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

fáceis

4.4. Assinaturas Digitais.

- a) Explique as diferenças entre a utilização das assinaturas digitais e os Message Authentication Codes, e porque oferecem garantias de segurança diferentes.

As assinaturas digitais baseiam-se na autenticação de uma mensagem através de cifração assimétrica, recorrendo a uma chave privada para autenticar a mensagem e uma chave pública para os verificar.

Os Message Authentication Codes autenticam uma mensagem através de cifra simétrica, sendo necessário a mensagem e chave secreta para verificar a mensagem. As assinaturas digitais são mais seguras do que os MAC, porque estas não necessitam do conhecimento da chave privada ou da mensagem. As assinaturas digitais providenciam autenticidade, integridade e não repúdio, ao que os MACs não providenciam não repúdio.

- b) A assinatura digital RSA Full Domain Hash calcula $\sigma = H(m)^d \bmod n$. Explique como funciona o processo de verificação da assinatura e como poderia ser quebrada no caso não se utilizar função de hash, calculando diretamente $\sigma = m^d$.

Para verificar a assinatura RSA Full Domain Hash, tem-se que decifrar o valor cifrado com a chave pública da entidade e verificar que o valor corresponde ao hash da mensagem. Se não fosse utilizado a função hash antes de assinar, obtia-se a mensagem original com a chave pública.

Grupo 5 - Protocolos e PKI (20%)

5.1. Cifras Autenticadas

- a) A cifra autenticada Encrypt-Then-MAC é (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-And-MAC é (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:

Como no Encrypt-And-MAC a chave usada é a mesma para cifrar e autenticar, então isso quer dizer que o output é determinístico, pois para a mesma chave obtém-se valores iguais. Como no IND-CPA as cifras tem que se indistinguíveis, então se estas forem produzidas através de um algoritmo determinístico, podem não ser indistinguíveis.

Uma cifra autenticada garante as propriedades de segurança .

- b) Explique como transformar a construção Encrypt-then-Mac num AEAD.

Para validar um certificado de chave pública que não raiz CA, primeiro realizam-se três validações básicas de identidade: se o certificado emitido pertence ao contexto de quem vou comunicar (e.g., DNS), se a entidade do certificado e metadados é quem vou comunicar (e.g., cliente) e se o certificado está valido diante o seu período de validade. Feitas estas três validações, e se estiverem válidas, segue-se para a validação da confiança com o emissor do certificado (CA). Validado esta, o último passo é verificar a assinatura digital com base na chave pública da CA.

- b) E como se valida um certificado de raiz?

A validação de uma certificado raiz é realizada implicitamente com o que é conhecido no cliente. No caso de um computador, este traz por defeito um conjunto de raiz de CA de forma a gerar uma caixa de confiança.

- c) Explique quantos certificados, no mínimo, são necessários para executar o protocolo Station-to-Station com autenticação mútua. Como são utilizados, e que garantias dão?

Station to Station = Full Authenticated Diffie-Hellman = Diffie-Hellman Anónimo + Verificação Trace

Para executar o protocolo Station-to-Station são necessários 4 certificados, 2 em cada lado da entidade. Estes são utilizados para garantir que num canal inseguro, a integridade das mensagens trocadas é cumprida, ao utilizar um certificado para iniciar a comunicação e verificar no outro lado