Primeiro teste de Criptografia Aplicada

24 de novembro de 2021 **16h00m – 18h00m**

1.0 **1:** As cifras contínuas, ou de fluxo (stream), são algoritmos praticáveis que permitem obter algo próximo de uma cifra de Vernam, também chamada de One-Time Pad. Explique:

i) Em que consiste uma cifra de Vernam; → chave aleatória, só pode ser usada uma vez com duas msg pode se obter a original

ii) Qual é o especial interesse da cifra de Vernam; → segurança absoluta

iii) Qual é a limitação da cifra de Vernam que as cifras contínuas habituais resolvem. → aleatoriedade da força da chave → stock de uma data enorme

1.0 **2:** Tendo em conta as 4 operações internas realizadas por uma cifra AES — AddRoundKey, SubBytes, ShiftRows, e MixColumns — quais são as que contribuem para concretizar o efeito de difusão, ou de avalanche? Justifique. → shift Rows/Colums, pq se muda com bit mude nem spot random

1.0 **3:** Imagine que se quer proteger de um potencial atacante que usa uma máquina com processamento paralelo, como uma unidade de processamento gráfico (GPU). Estas unidades são particularmente rápidas quando executam exatamente as mesmas instruções sobre dados diferentes. Assumindo que o atacante tem de experimentar várias chaves e decifrar as mensagens-alvo completamente de forma a verificar se escolheu a chave certa, que modo de cifra escolheria? Justifique a sua resposta. → OFB, Não tem random access só se processar o Ek de todo previamente mas tbm muitos recursos

1.0 **4:** É correto afirmar que o modo de cifra CBC concretiza uma cifra polialfabética? Justifique. → sim visto como o bloco anterior influencia o próximo mas só sabe qual o final logo um mesmo de entrada pode ter vários outputs

1.0 **5:** Considere as 3 formas normais de combinar cifra e controlo de integridade de uma mensagem: Encrypt-then MAC, Encrypt-and-MAC e MAC-then-encrypt. Indique, justificadamente, qual é a pior e a melhor, em termos de tempo de processamento gasto, para verificar se recebeu uma mensagem inválida (adulterada ou fabricada). Nota: assuma que os algoritmos de cifra e de controlo de integridade são independentes. → Encrypt-then-MAC, melhor pq só tem de computar o Enc com o MAC pior MAC-then-Encrypt, pq o tempo de descriptar e comparar é maior que MAC and Enc

1.0 **6:** Para que é que serve o protocolo de Diffie-Hellman? Qual é o problema matemático que o torna criptograficamente "seguro"? → key exchange, só com r, p, A, B ó fácil encontrar α, β, S a partir de α, β

1.0 **7:** O protocolo Diffie-Hellman também pode ser implementado usando curvas elípticas. Explique como. Aproveite a ocasião para explicar muito resumidamente que operações aritméticas podem ser feitas sobre pontos pertencentes a uma curva elíptica. → P, célica, e ambos o seu $K_A P = A$, $K_B P = B$ depois $K_A B = K_B A = K_A K_B P$ sabendo $K_A P$ ó fácil encontrar K_A

1.0 **8:** O sistema criptográfico RSA pode ser usado para cifrar uma mensagem. Explique como. Qual é o problema matemático que o torna criptograficamente "seguro"? → $ed = 1 \bmod \lambda(pq)$, pois se calcular λ tem de saber p e q mas com pq ó difícil descobrir p e q separados $m^e \pmod{pq} = c$ $c^d \pmod{pq} = m$

1.0 **9:** O sistema criptográfico RSA pode também ser usado para assinar uma mensagem, isto é, para atestar, desde que sejam tomadas as precauções devidas, que uma messagem não foi forjada por outro que não o remetente. Explique como. → Faz o MAC enc com a priv e depois alguém sabe o MAC compara com o MAC dec com pub e fz

1.0 **10:** Suponha que o número $\boldsymbol{M}$ que codifica uma mensagem que vai ser cifrada pelo RSA é, por azar, múltiplo de um dos fatores do módulo. Suponha ainda que a mensagem cifrada é interceptada. Quando isso acontece, que informação é revelada? Se for revelada alguma informação, isso é ou não um problema sério para o uso generalizado deste método de cifra?