As notas de aula tem vários exercícios; selecionei alguns que poderiam ser incluídos na prova. A prova poderá ter também questões conceituais e de outros tipos.

Ex. 1 — Mostre que a função de adição $f(x, y) = x + y$ (x e y tem a mesma quantidade de bits) não é de mão única.

Ex. 2 — O modo CBC de encriptação corrige erros no texto decriptado. Mostre que se há um erro no bloco c_j, mas todos os outros blocos são transmitidos corretamente, apenas dois serão afetados (mostre quais).

Ex. 3 — Mostre que é possível decriptar a saída de uma rede de Feistel encriptando o texto cifrado, mas revertendo a ordem das subchaves usadas em cada rodada.

Ex. 4 — Crie uma S-box com 4 bits de entrada e 4 de saída que, assim como o `SubBytes` do AES, não tenha ponto fixo.

Ex. 5 — Explique porque o ataque do encontro no meio não funciona para $F'_{k_1,k_2,k_3} = F_{k_1}(F^{-1}_{k_2}(F_{k_3}(m)))$.

Ex. 6 — Considere o seguinte Criptossistema: as mensagens tem 32 bits, e são interpretadas como números de 32 bits.

- $\texttt{Gen}(1^n)$ escolhe aleatoreamente um número de 32 bits
- $\texttt{Enc}_k(m) = m + k \pmod{32}$
- $\texttt{Dec}_k(c) = c - k \pmod{32}$

A soma e subtração módulo 32 já existem de graça em CPUs (basta usar soma normalmente – a CPU faz $\pmod{32}$).

a) Prove que o criptossistema funciona.

b) O sistema tem segurança contra múltiplos textos encriptados? Caso tenha, explique porque; caso não tenha, sugira uma forma de "consertá-lo".