Quiz 3

1. As with Rijndael, suppose we are working in the finite field with 2^8 elements, representing field points using the irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$ Compute the byte which is the result of multiplying bytes:

$$'\texttt{E1}' \bullet '\texttt{03}'$$

   That is, the first byte, `11100001` in binary, corresponds to polynomial $x^7 + x^6 + x^5 + 1$; while the second byte, `00000011` in binary, corresponds to the polynomial $x + 1$. You are to find the byte which is the product.

2. Block cipher DES has 56-bit keys and a 64-bit blocksize: DES : $\{0,1\}^{56} \times \{0,1\}^{64} \to \{0,1\}^{64}$.

   - How many different DES keys are possible?

   - Here is the number of permutations on 64-bits (that is, $|\mathrm{Perm}(n)|$):

   - At most how many different values for $\mathrm{DES}_K(\mathbf{0})$ are possible (here $\mathbf{0} = 0^{64}$)?

   - Clearly define an adversary A, having oracle f, that asks one query and gets advantage $\mathbf{Adv}^{\mathrm{prp}}_{\mathrm{DES}}(A) \geq 255/256$.

3. About how many random 80-bit strings $x_1, x_2, \ldots$ do you need to choose until you expect to see the first "collision": some $x_i = x_j$, where $i \neq j$.

4. **Definition.** Let A be an adversary attacking the symmetric **encryption scheme** $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$. Then

$$\mathbf{Adv}^{\mathrm{rr}}_{\Pi}(A) \;=$$

End of quiz!