



Problem 3. «Hash function FNV-1a»

Hash function **FNV-1a** processes a message x composed of bytes $x_1, x_2, \dots, x_n \in \{0, 1, \dots, 255\}$ in the following way:

- 1) $h \leftarrow h_0$;
- 2) for $i = 1, 2, \dots, n$: $h \leftarrow (h \oplus x_i)g \bmod 2^{128}$;
- 3) return h .

Here $h_0 = 144066263297769815596495629667062367629$, $g = 2^{88} + 315$. The expression $h \oplus x_i$ means that the least significant byte of h is added bitwise modulo 2 with the byte x_i .

Find a collision, that is, two different messages x and x' such that $\text{FNV-1a}(x) = \text{FNV-1a}(x')$. Collisions on short messages and collisions that are obtained without intensive calculations are welcomed. Supply your answer as a pair of two hexadecimal strings which encode bytes of colliding messages.

