decrypt - solution

There are 2 phases:

1. Determine R[0], R[1], R[2]
2. Determine M[0], M[1], …, M[255]

- *Phase 1*.

Solving this problem starts by observing that R has a period of 7 (or 1 iff R[0] = R[1] = R[2] = 0).

Also xor is a bitwise operation so the 8 bits of each R are independent. We are only interested in finding out a bit for now (let's assume least significant bit). The other bits are computed in a similar fashion.

Let R[0] = a, R[1] = b, R[2] = c, where a, b, c are bits.
R[3] = a xor b
R[4] = b xor c
R[5] = a xor b xor c
R[6] = a xor c

We start to play with the encryption device. What we ask is not that important, but we have to make sure that we don't ask the same number after 7*P uses, because we would just waste a query.

What we care about are **collisions**, i.e. 2 queries that give the same answer.

Let Q1, Q2 be the queries we asked at times T1 and T2, respectively.

Since M[Q1 XOR R[T1]] = M[Q2 XOR R[T2]] and M is a permutation we deduce that R[T1] XOR Q1 = R[T2] XOR Q2. This is the same as R[T1] XOR R[T2] = Q1 XOR Q2.

This pretty much gives an equation for finding out a, b and c.

What we need is 3 independent equations (independent collisions). We can continue to play with the device until we get them. Some attention is needed to make sure the equations are really independent.

Once we have 3 independent collisions we can find out a, b, c.

We can do the same for the rest of the bits: 1 through 7. We just have to use a different bit from Q1 XOR Q2.

- *Phase 2.*

Now that we know R[0], R[1] and R[2] we can compute M. It's important to remember the queries from step (1), otherwise the number of queries can easily exceed 320.

We know the step we are at (N) and the element of M that we want to compute. Let X be the index of the element. We query for R[N] XOR X. This gives us M[X].

The total number of queries should be at least 256 (for M) and 3 (for 3 collisions). However many collisions are not independent. Since the tests are random it's easy to find 3 independent collisions in at most 32 collisions.