giả lập mã hóa One-Time pad. Đây là cơ sở thực hiện của mã dòng (stream cipher).

- Một khối được mã hóa bằng phép XOR với khóa. Điều này không an toàn vì chỉ cần biết *một cặp khối* bản rõ - bản mã (vd: 1111 và 1010), người phá mã dễ dàng tính được khóa. Để khắc phục điều này, người ta tìm ra các phép mã hóa phức tạp hơn phép XOR, và đây là cơ sở ra đời của mã khối (block cipher).

3.1 Mã dòng (Stream Cipher)

Mã dòng có các đặc tính sau:

- Kích thước một đơn vị mã hóa: gồm k bít. Bản rõ được chia thành các đơn vị mã hóa: $P \rightarrow p_0 p_1 p_2 \dots p_{n-1} \quad (p_i : k\ bít)$
- Một bộ sinh dãy số ngẫu nhiên: dùng một khóa K ban đầu để sinh ra các số ngẫu nhiên có kích thước bằng kích thước đơn vị mã hóa: $StreamCipher(K) \rightarrow S = s_0 s_1 s_2 \dots s_{n-1} \quad (s_i : k\ bít)$
- Mỗi số ngẫu nhiên được XOR với đơn vị mã hóa của bản rõ để có được bản mã.

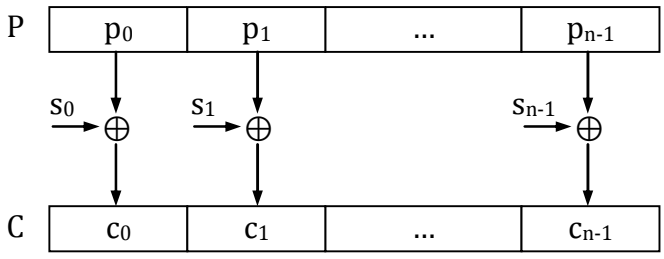
$$c_0 = p_0 \oplus s_0,\ c_1 = p_1 \oplus s_1 \dots \ ; C = c_0 c_1 c_2 \dots c_{n-1}$$

Quá trình giải mã được thực hiện ngược lại, bản mã C được XOR với dãy số ngẫu nhiên S để cho ra lại bản rõ ban đầu: $p_0 = c_0 \oplus s_0,\ p_1 = c_1 \oplus s_1 \dots$

Trong ví dụ trên đơn vị mã hóa có chiều dài k = 4 bít, n = 3:

$$p_0 = 1111,\ p_1 = 0000,\ p_2 = 0011$$
$$s_0 = s_1 = s_2 = K = 0101$$
$$c_0 = 1010,\ c_1 = 0101,\ c_2 = 0110$$

Ví dụ này không phải là mã dòng vì s_0, s_1, s_2 lặp lại khóa K. Về phương diện khóa, ví dụ này giống mã Vigenere hơn. Đối với mã dòng, các số s_i được sinh ra phải đảm bảo một độ ngẫu nhiên nào đó (chu kỳ tuần hoàn dài):



Hình 3-1. Mô hình mã dòng

Như vậy có thể thấy mã hóa dòng tương tự như mã hóa Vigenere và mã hóa One-Time Pad. Điểm quan trọng nhất của các mã dòng là bộ sinh số ngẫu nhiên. Nếu chọn khóa có chiều dài ngắn như mã hóa Vigenere thì không bảo đảm an toàn, còn nếu chọn khóa có chiều dài bằng chiều dài bản tin như One-Time Pad thì lại không thực tế. Bộ sinh số của mã dòng cân bằng giữa hai điểm này, cho phép dùng một khóa ngắn nhưng dãy số sinh ra bảo đảm một độ ngẫu nhiên cần thiết như khóa của One-time Pad, dùng rằng không hoàn toàn thực sự ngẫu nhiên.