Giải mã Playfair dựa vào sự liên quan của các chữ cái nên việc xác định các xâu bản rõ ứng cử viên dễ dàng hơn. Đặc biệt là chữ ghép Playfair và ngược của chữ ghép đó (ví dụ AB và BA) sẽ giải mã thành cùng một kiểu mẫu chữ cái trong bản rõ (Ví dụ RE và ER). Trong tiếng Anh, có rất nhiều từ chứa những bộ chữ ghép ngược này như REceivER và DEpartED. Việc xác định những bộ chữ ghép ngược mà gần nhau trong bản mã và ghép kiểu mẫu thành một danh sách các từ rõ đã biết chứa kiểu mẫu là đơn giản từ đó đưa ra được các xâu bản rõ có thể rồi sẽ xác định khóa.

Một cách tiếp cận khác là phương pháp Shotgun hill climbing. Bắt đầu với hình vuông các chữ cái ngẫu nhiên sau đó thực hiện những sự thay đổi nhỏ (ví dụ như chuyển các chữ cái, các hàng hay phản xạ toàn bộ hình vuông) để thấy được nếu bản rõ ứng cử viên giống bản rõ chuẩn hơn so với trước khi thay đổi (có thể bằng cách so sánh các nhóm ba thành lược đồ tần suất đã biết). Nếu hình vuông mới có sự cải tiến thì nó sẽ được chấp nhận và sau sẽ được biến đổi thêm để tìm ra một ứng cử viên tốt hơn. Cuối cùng là dù chọn phương pháp phân loại nào thì cũng tìm ra bản rõ hoặc một văn bản rất gần bản rõ với khả năng đúng là lớn nhất. Máy tính có thể chấp nhận thuật toán này để phá các mật mã Playfair với số lượng văn bản tương đối nhỏ.

Phương pháp Playfair thường được áp dụng trong việc giải các trò chơi đố các ô chữ.

2.3. Mã dòng

Trong các hệ mật trên, các phần tử rõ được mã hoá bằng cách dùng *cùng một khoá*k:

$y = y_1\ y_2 \ldots y_n = e_k(x_1)\ e_k(x_2) \ldots e_k(x_n)$

Ở đây x_i có thể là một hoặc một dãy ký tự.

Hệ mật loại này được gọi là mật mã khối, hay đơn giản là mã khối.Bây giờ ta nghiên cứu mật mã dòng. Ý tưởng cơ bản là sinh dòng khoá:

$z = z_1\ z_2 \ldots$ và mã hóa dòng rõ $x = x_1\ x_2 \ldots$ theo cách:

$y = y_1 y_2 \ldots = e_{z_1}(x_1) e_{z_2}(x_2) \ldots$

Mật mã dòng hoạt động như sau:

+ Giả sử k là khoá và $x_1 x_2 \ldots$ là dòng rõ, f_i là hàm của k và i – 1 đặc trưng rõ:

$z_i = f_i(k, x_1, \ldots, x_{i+1})$, x_1được chọn trước bởi hai bên.

$y_i = e_{z_i}(x_i)$, i = 2, 3,...

Do đó để mã hóa dòng rõ $x_1 x_2 \ldots$, ta tính liên tiếp:

$z_1, y_1, z_2, y_2 \ldots$

Việc giải mã được làm tương tự:

$z_1, x_1, z_2, x_2 \ldots$

Nếu $z_i = k$ với mọi i, thì ta có thể nghĩ mật mã khối như trường hợp đặc biệt của mật mã dòng. Sau đây là một số trường hợp đặc biệt nhưng quan trọng của mật mã dòng:

- Mật mã đồng bộ: $z_i = f_i(k)$ i = 1, 2, ...

- Mật mã tuần hoàn với chu kỳ d: $z_{i+d} = z_i$, với mọi i >= 1

Mật mã dòng được chú ý nhiều là trường hợp $P = C = Z_2$. Khi đó phép mã hoá và giải mã là cộng theo modulo 2:

$e_z(x) = x + z \bmod 2$

$d_z(x) = y + z \bmod 2$

Khoá được sinh theo phương pháp ghi dịch phản hồi.

- Mật mã khoá tự động:

$P = C = K = Z_{26}$

$Z_1 = k$, $Z_i = x_{i-1}$ (i >= 2)

$e_z(x) = x + z \bmod 2$

$d_z(x) = y - z \bmod 2$; với $x, y \in Z_{26}$

Ví dụ:

K = 8, thông báo cần mã là: hairphongf

Trước tiên, chuyển thông báo rõ thành dãy số nguyên:

7 0 8 17 15 7 14 13 6 5

Dòng khoá như sau:

8 7 0 8 17 15 7 14 13 6 5

Cộng dãy khoá và dãy rõ theo qui tắc: $y_i = x_i + z_i \bmod 26$ i = 1, 2, ...

ta được:

15 7 8 25 6 22 21 1 19 11

và chuyển thành chữ:

p h i z g w v b t l

Với bản mã này và k = 8, ta giải mã như sau:

- Chuyển dãy mã thành số và trừ lần lượt

15	**7**	**8**	**25**	**6**	**22**	**21**	**1**	**19**	**11**
8	**7**	**0**	**8**	**17**	**15**	**7**	**14**	**13**	**6**
7	**0**	**8**	**17**	**15**	**7**	**14**	**13**	**6**	**3**

- Chuyển dãy số thành dãy chữ: h a i r p h o n g f

2.4. Mã khối

2.4.1. Giới thiệu chung

Các hệ mật khóa bí mật thường được chia thành các hệ mã khối và hệ mã dòng. Đối với mã khối bản rõ có dạng các khối "lớn" (chẳng hạn 128-bit) và dãy các khối đều được mã bởi cùng một hàm mã hóa, tức là bộ mã hóa là một hàm không nhớ. Trong mã dòng, bản rõ thường là dãy các khối "nhỏ" (thường là 1-bit) và được biến đổi bởi một bộ mã hóa có nhớ.

Các hệ mã khối có ưu điểm là chúng có thể được chuẩn hóa một cách dễ dàng, bởi vì các đơn vị xử lý thông tin hiện này thường có dạng block như bytes hoặc words.

Nhược điểm lớn nhất của mã khối là phép mã hóa không che giấu được các mẫu dữ liệu: các khối mã giống nhau sẽ suy ra các khối rõ cũng giống nhau. Tuy nhiên nhược điểm này có thể được khắc phục bằng cách