Cifrul Playfair

Pentru a cripta un mesaj avem nevoie de text clar și cheie. Folosind cheia formăm careul Polybios 5x5 sau 6x6 și împărțim textul clar în bigrame. Dacă într-un bigram caracterele sunt egale, atunci se introduce X sau alt caracter rar utilizat în locul caracterului duplicat, care se introduce mai departe. Dacă șirul se sfârșește cu 1 caracter, atunci se formează un bigram din caracterul dat și X.

Mai departe folosim careul format pentru a cripta bigramele. Dacă caracterele sunt în același rând, atunci se ia caracterul din dreapta relativ de fiecare char. Analog, dacă caracterele sunt în aceeași coloană, atunci luăm caracterele respective cu 1 rând mai jos. Dacă caracterele sunt din rânduri și coloane diferite, atunci acestea se înlocuiesc cu caracterele din același rând, dar coloana corespunzătoare celuilalt caracter din bigramul inițial. În final bigramele obținute se unesc, astfel formând textul criptat.

Procedura de decriptare este inversă celei de criptare: folosim cheia pentru a forma careul 5x5 sau 6x6 și decriptăm bigramele invers algoritmului de mai sus, apoi unim bigramele obținute ca să primim textul clar.