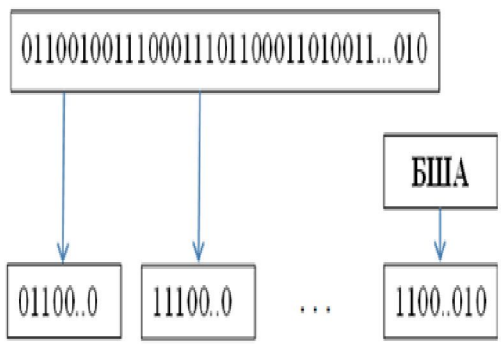
[2]. X.Chen, H.White, Central limit and functional central limit theorems for Hilbert-valued dependent heterogeneous arrays with applications. Econometric Theory 14,(1998), 260-284.

[3]. F. Hofbauer, G.Keller, Ergodic properties of invariant measures for piecewise monotonic transformations. Math.Z.180,(1982), 119-142.

БЛОКЛИ ШИФРЛАРНИ ҚУРИШ ПРИНЦИПЛАРИ

Шермухаммедов Ж.А.
Ўзбекистон Миллий Университети
e-mail: shaxnur.samadov92@mail.ru

Фараз қилайлик, шифрланиши лозим бўлган хабар ноль ва бирлардан иборат кема-кетлик, яъни иккилик кўринишида ифодаланган бўлсин. Агар шифрлаш жараёнидан олдин ушбу кетма-кетлик фиксирланган узунликдаги блокларга бўлинса ва ушбу блоклар алоҳида шифрланса, бундай шифрланиш жараёни блокли шифрлаш деб номланади. Шифрланиш жараёнида қўлланилган шифр эса блокли шифр дейилади (1-расм).

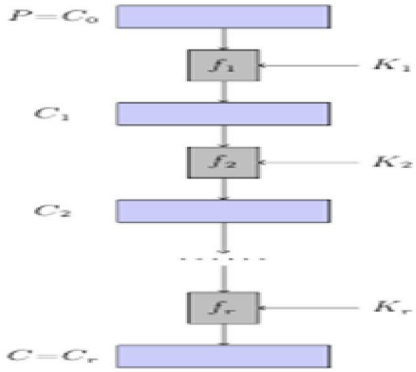


1-расм. Блокли шифрлаш.

Ҳар блокни очиқматн (инглиз тилида *plaintext*) деб номлаш ва уни P билан белгилаш қабул қилинган. Одатда блокларни ўлчови сифатида 64, 128 ва 256 битлардан ташкил топган кетма-кетликлар узунликларидан фойдаланилади [1,2].

m узунликдаги битларнинг махфий кетма-кетлиги K (key) шифрлаш калити деб номланади. Замонавий шифрлаш алгоритмлари калитларининг узунликлари 128, 256 ва 512 битлар кетма-кетлигидан ташкил топган.

Ҳар бир блокли шифрни асосини шифрлаш калити турли битлари билан боғлиқбўлган бир хил криптографик алмаштириш ва амалларни бир неча марта такрорлаш ташкил қилади. Ушбу такрорланишлар сони блокли шифрнинг раундлари деб аталади. Блокли шифрлар шундай тарзда қуриладики, i-чи раунд натижасида ҳосил қилинган C_i шифрматн i+1-чи раунд учун кирувчи хабар вазифасини ўтайди (2-расм). Охирги раунддан ҳосил қилинган шифрлаш натижаси шифрматн ҳисобланади: $C_r = C$.



2-расм. Блокли шифрларни умумий кўриниши.

Блокли шифрларни амалдаги раундлар сони $r = 8 \div 64$. Блокли шифрлашни тезлигини ошириш мақсадида r=8 ва унинг юқори криптобардошлигини таъминлаш масадида r=64 каби раундларнинг мос ҳолда кичик ва катта сонларидан фойдаланилади [1,2].

Фойдаланилган адабиётлар

[1]. Панасенко С. П. Алгоритмы шифрования. Специальный справочник. СПб.: БХВ-Петербург, 2009. 576 с.

[2]. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф. 2002. 816 с.

ФОРМУЛА КАРЛЕМАНА ДЛЯ ПОТЕНЦИАЛЬНОГО ВЕКТОРА В ОБЛАСТИ ТИПА КОНУСА

Эрмаматова З.Э.
Самаркандский государственный университет
e-mail: Sattorov-e@rambler.ru

В работе рассматривается задача восстановления решения обобщенной системы Коши-Римана в многомерной пространственной области по их значениям на куске границы этой области, т.е. задача Коши. Строится приближенное решение этой задачи, основанное на методе матрицы Карлемана.

Ключевые слова: уравнения Коши-Римана, некорректные задачи, регулярное решение, матрица Карлемана.

1. Обозначения и постановка задачи

R^3 - трехмерное вещественное евклидово пространство: $x = (x_1, x_2, x_3)$, $y = (y_1, y_2, y_3) \in R^3$, $x' = (x_1, x_2)$, $y' = (y_1, y_2) \in R^2$, $\alpha = |y' - x'|$, $\alpha^2 = s$, $r^2 = |y - x|^2 = \alpha^2 + (y_3 - x_3)^2$, $\tau = tg\frac{\pi}{2\rho}$, $\rho > 1$, $G_\rho = \{y : |y'| < \tau y_1,\ y_1 > 0\}$, $\partial G_\rho = \{y : |y'| = \tau y_1,\ y_1 > 0\}$, $\overline{G}_\rho = G_\rho \cup \partial G_\rho$, $\varepsilon, \varepsilon_1, \varepsilon_2-$ достаточно малые постоянные положительные числа, $G_\rho^\varepsilon = \{y : |y'| < \tau(y_1 - \varepsilon)\}$, $\partial G_\rho^\varepsilon = \{y : |y'| = \tau(y_1 - \varepsilon)\}$ $\overline{G}_\rho^\varepsilon = G_\rho^\varepsilon \cup \partial G_\rho^\varepsilon$,

$$C = \{\varsigma : \varsigma = \xi + i\eta,\ -\infty < \xi < \infty,\ -\infty < \eta < \infty, \}.$$