Noekeon

Криптоалгоритм $Noekeon$[1] шифрует 128-битовые блоки открытых данных под управлением секретного ключа такого же размера. Алгоритм существует в двух режимах: прямом (direct mode) и косвенном (indirect mode). Разница между ними – в расширении ключа. Здесь рассматривается только прямой режим.

Блок шифруемых данных P и секретный ключ K представляются в виде конкатенации четырех 32-битовых слов: $P = P_0P_1P_2P_3$ и $K = K_0K_1K_2K_3$. В алгоритме используется преобразования со следующими логическими операциями над 32-битовыми словами a и b:

$\neg\, a$ – побитовое отрицание a;

$a \,\&\, b$ – побитовое умножение a и b;

$a \vee b$ – побитовая дизьюнкция a и b;

$a \oplus b$ – побитовое сложение a и b по модулю 2;

$shl_n\ a$ ($shr_n\ a$) – сдвиг a влево (право) на n позиций.

$rol_n\ a$ ($ror_n\ a$) – циклический сдвиг a влево (право) на n позиций.

Преобразования θ определяется как:

$\theta(K, P) \equiv \{$
$\quad t := P_0 \oplus P_2;$
$\quad S(t);$
$\quad P_1 := P_1 \oplus t;$
$\quad P_3 := P_3 \oplus t;$
$\quad (P_0, P_1, P_2, P_3) := (P_0 \oplus K_0, P_1 \oplus K_1, P_2 \oplus K_2, P_3 \oplus K_3);$
$\quad t := P_1 \oplus P_3;$
$\quad S(t);$
$\quad P_0 := P_0 \oplus t; P_2 := P_2 \oplus t$
$\},$

где

$S(t) \equiv \{t := t \oplus shr_8\ t \oplus shl_8\ t\}.$

Обратное преобразование θ^{-1}, возвращающее P к исходному значению, задаётся следующим образом:

$\theta^{-1}(K, P) \equiv \{$
$\quad t := P_1 \oplus P_3;$
$\quad S(t);$
$\quad P_0 := P_0 \oplus t;$
$\quad P_2 := P_2 \oplus t;$
$\quad (P_0, P_1, P_2, P_3) := (P_0 \oplus K_0, P_1 \oplus K_1, P_2 \oplus K_2, P_3 \oplus K_3);$
$\quad t := P_0 \oplus P_2;\ S(t);\ P_1 := P_1 \oplus t; P_3 := P_3 \oplus t$
$\}.$

Отметим также, что $\theta^{-1}(K, P) = \theta(K^{(d)}, P)$, где $K^{(d)}$ получается из K применением преобразования θ с нулевым ключом, т.е. $\theta(0, K)$.

Преобразования γ, π_1 и π_2 определяются как

$\gamma(P) \equiv \{$
$\quad P_1 := P_1 \oplus \neg(P_2 \vee P_3);$
$\quad P_0 := P_0 \oplus (P_1 \& P_2);$
$\quad P_0 \leftrightarrow P_3;$
$\quad P_2 := P_0 \oplus P_1 \oplus P_2 \oplus P_3;$
$\quad P_1 := P_1 \oplus \neg(P2 \vee P3);$
$\quad P_0 := P_0 \oplus (P_1 \& P_2)$
$\}.$

$\pi_1(P) \equiv \{rol_1 P_1; rol_5 P_2; rol_2 P_3\}.$

---

[1] Авторы шифра: *Joan Daemen*, *Michael Peeters*, *Gilles Van Assche* и *Vincent Rijmen* (Бельгия)

$\pi_2(P) \equiv \{ror_1 P_1; ror_5 P_2; ror_2 P_3\}$.

Отметим, что $\gamma^{-1} = \gamma$; $\pi_1^{-1} = \pi_2$, $\pi_2^{-1} = \pi_1$.

Алгоритм зашифрования *Noekeon*

Вход: P – 128-битовый блок открытых данных.

for $i := 1$ ***to*** R ***do*** {
    $\theta(K, P)$;
    $\pi_1(P)$;
    $\gamma(P)$;
    $\pi_2(P)$
};
$\theta(K, P)$.

Выход: P – 128-битовый шифртекст. Стандартное число раундов $R = 16$.

Этот же алгоритм используется и для расшифрования, но при этом необходимо заменить либо θ на θ^{-1}, либо K на $K^{(d)}$ (одно из двух).