Kötelező félévi házi feladat (Modellellenőrzés)

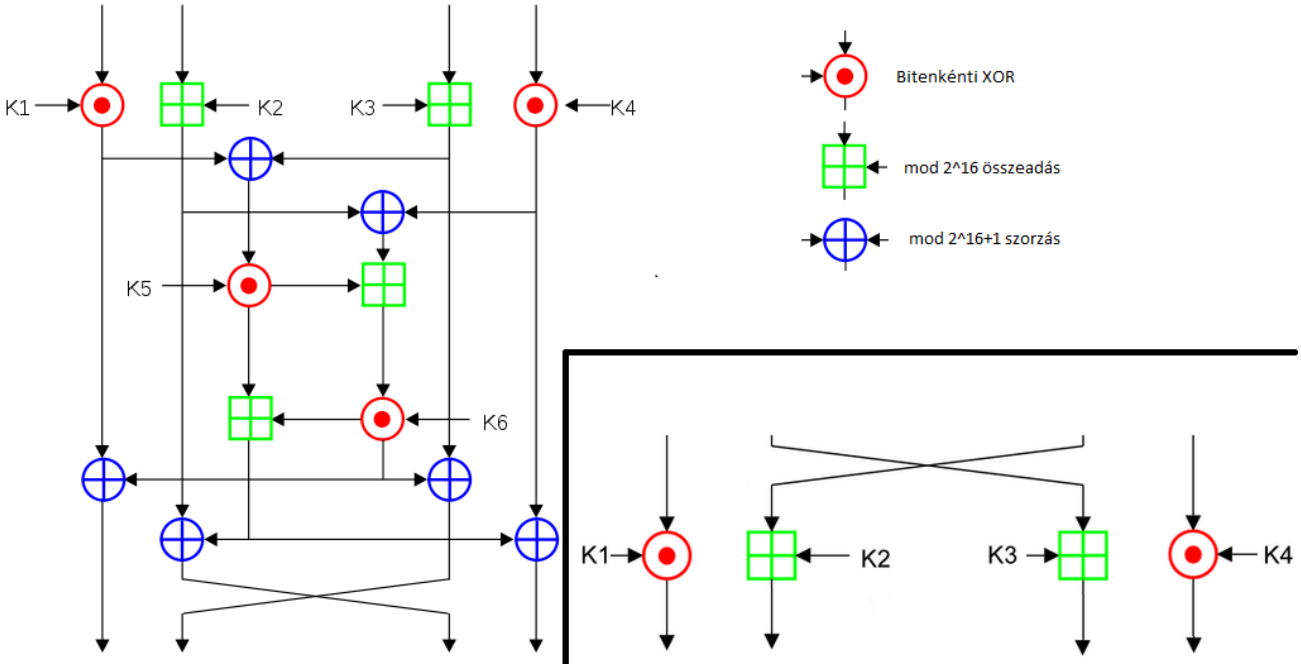
A feladat címe: **Titkosító modul**

Konzulense: **Hegedüs Ábel**

Leírás

A bizalmas adatok védelmének egyik alapvető módja a titkosítás használata. Sokféle titkosító algoritmus és szoftveres vagy hardveres titkosító komponens használható, ezek közül a házi feladat során az IDEA[1] elnevezésű algoritmust implementáló, valós idejű üzenetek titkosítását támogató komponens modellezése a feladat.

A komponenst fejlesztő vállalatnak biztosítania kell azt, hogy mind a titkosítás megfelelően működjön, mind azt, hogy az adatátvitel megfelelően gyors. Az IDEA egy szimmetrikus blokk kódoló, így ugyanaz a komponens használható kódoláshoz és dekódoláshoz, továbbá az adatok kezelése adott nagyságú blokkonként történik. Az IDEA algoritmusban egy alap transzformáció (menet) többszöri egymás után illesztésével érhető el a megfelelő titkosítási szint. Az alábbi ábrákon látható az IDEA menet, amelyből az eredeti algoritmusban 8-t használnak, valamint az IDEA félmenet, amelyet utolsóként használnak a kimenet előállítására.



1. ábra IDEA kódoló menet és félmenet

A kódoló bemenetén 64 bites blokkokat fogad, amelyeket egy 128 bites kulcs segítségével titkosítja, szintén 64 bites kimenetet generálva. A bemenetet négy 16 bites részre bontja, a kulcsot pedig szintén 16 bites részenként használja, körönként hatot (következő körökben mindig a legutóbb használt rész után következőt, így biztosítva a megfelelő keverést). Az eredeti algoritmusban a kulcsot forgatják is (bitenként eltolják), de ezt nem kell modellezni.

[1] http://en.wikipedia.org/wiki/International_Data_Encryption_Algorithm

Előzetes mérések során kiderült, hogy az egyes operációk (xor, mod összeadás, mod szorzás) időigénye különböző. A bitenkénti XOR művelet 1 ms, a mod 2^{16} összeadás és a mod $2^{16}+1$ szorzás pedig 4 ms időt igényel. Egy művelet akkor hajtható végre, ha mindkét bemenete és a szükséges erőforrás rendelkezésre áll (de akkor azonnal, nincs várakozás). A számoláshoz több erőforrás rendelkezésre áll, amelyek segítségével lehetőség van több menetet egyszerre futtatni (például amikor a kezdeti bemenettel végzett az első menet, akkor a következő bemenetblokkot kezdheti el, míg a második menet fut az első menet kimenetén). Fontos, hogy nem biztos, hogy annyi erőforrás van, ahány menetet el kell végezni.

Egy konkrét IDEA komponenst a következő paraméterekkel írunk le: bemenet mérete (blokkszám), teljes menetek száma, rendelkezésre álló XOR, mod összeadó és mod szorzók száma.

Amikor a teljes kimenet előállt egy adott blokkszámú bemenetre, akkor kezdődhet a következő bemenet feldolgozása.

Az ellenőrzendő követelmények

Temporális logikai kifejezések és modellellenőrzés segítségével igazolja az alábbi követelmények teljesülését (illetve a követelmények nem teljesülése esetén ellenpélda segítségével magyarázza meg a követelmény megsértésének okát és indokát)!

1. A modellben nincs deadlock. (paraméterek: 1; 1; 1; 1; 1)
2. A teljes kimenet előállítása megtörténik 300 ms alatt. (paraméterek: 3; 2; 4; 2; 2)
3. Mindig igaz, hogy a kimeneten szereplő adat a bemenet minden részétől függ. (paraméterek: 1; 2; 3; 2; 2)
4. A kulcs minden részét felhasználja az algoritmus minden menetben. (paraméterek: 1; 2; 1; 1; 1)