Óbudai Egyetem

Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

Műszaki területek informatikai biztonsága

Kulcscsere protokollok

ZENTAI DÁNIEL

ZENTAI.DANIEL@BGK.UNI-OBUDA.HU

Kulcscsere protokollok

Szimmetrikus kulcsú titkosításoknál el kell juttatni a kulcsot valamilyen biztonságos csatornán a kommunikáló felekhez.

Követelmények:

A kommunikáló felekhez ugyanaz a kulcs jusson el. (effektivitás)

Senki más ne tudja meg a kulcsot. (kulcs hitelesítés)

A kulcs frissen generált legyen. (kulcs frissesség)

Ha Alice és Bob beszélgetnek, akkor Alice meg tud győződni arról, hogy Bob tudja a kulcsot, és fordítva. (kulcs megerősítés)

Kulcscsere protokollok

Kétféle kulcscsere protokollt ismerünk:

Kulcs transzport:

Az egyik résztvevő fél (esetleg egy megbízható szerver) generál egy kulcsot, és ezt továbbítja a többi résztvevőnek.

Kulcs megegyezés:

A kulcs a résztvevő felek által birtokolt információnak valamilyen együttes függvénye

Kulcs megegyezés:

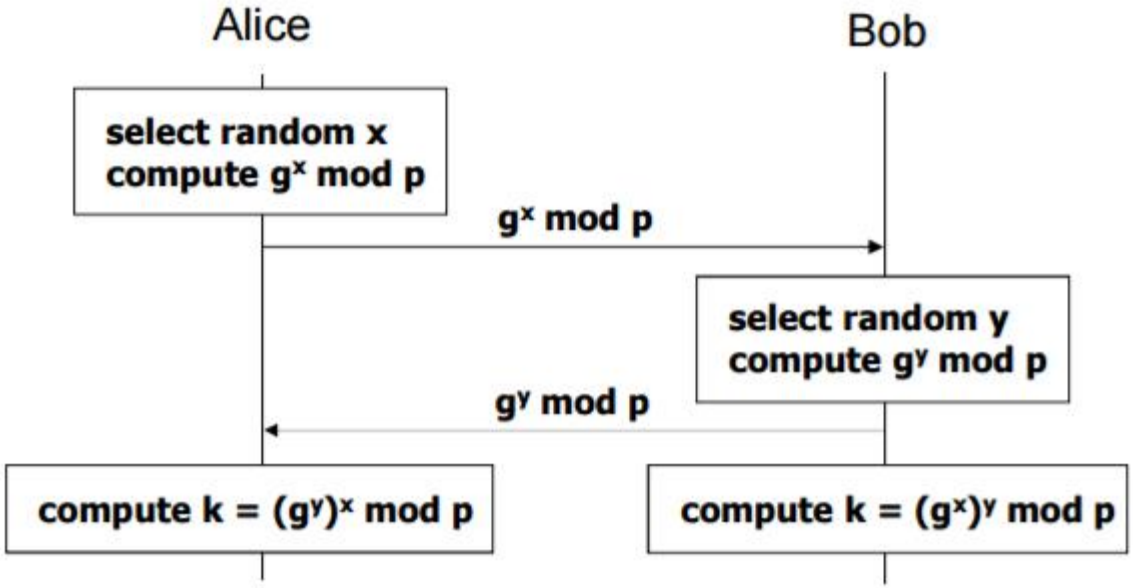
A kulcs kiszámítása: $K = f(k_A , k_B)$

Követelmény: $f(k_A , .)$ bármely fix k_A esetén egyirányú függvény, azaz miután Alice választott egy k_A értéket, Bob ne tudjon olyan k_B értéket választani, hogy $f(k_A , k_B)$ valamely előre definiált érték legyen. Más szavakkal bármely fix k_A esetén $f(k_A , k_B)$ ismeretében nehéz feladat k_B kiszámítása.
Ugyanez igaz bármely fix k_B –re is.

Ilyen például a diszkrét logaritmus probléma.

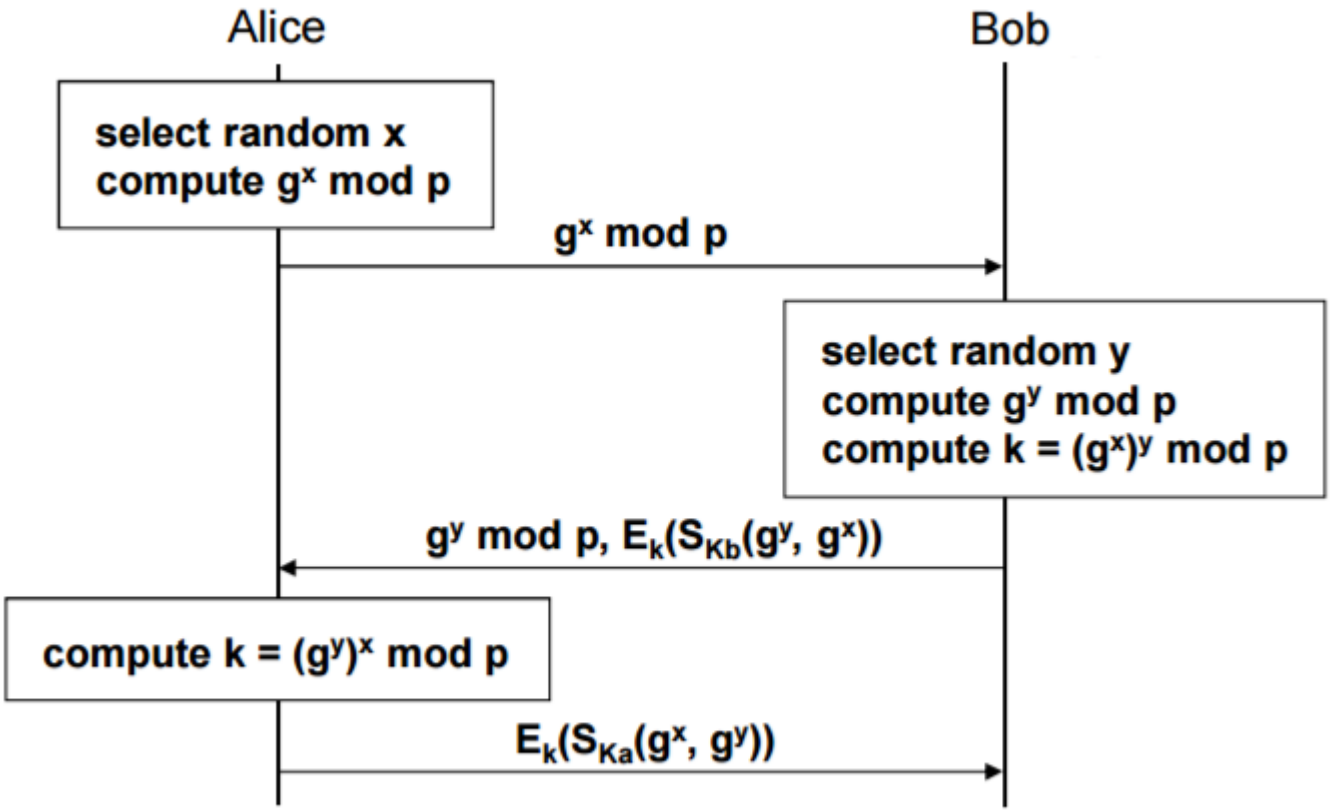
A Diffie-Hellman protokoll

Publikus adatok: G ciklikus csoport, |G| = p prím, g generátoreleme G-nek.

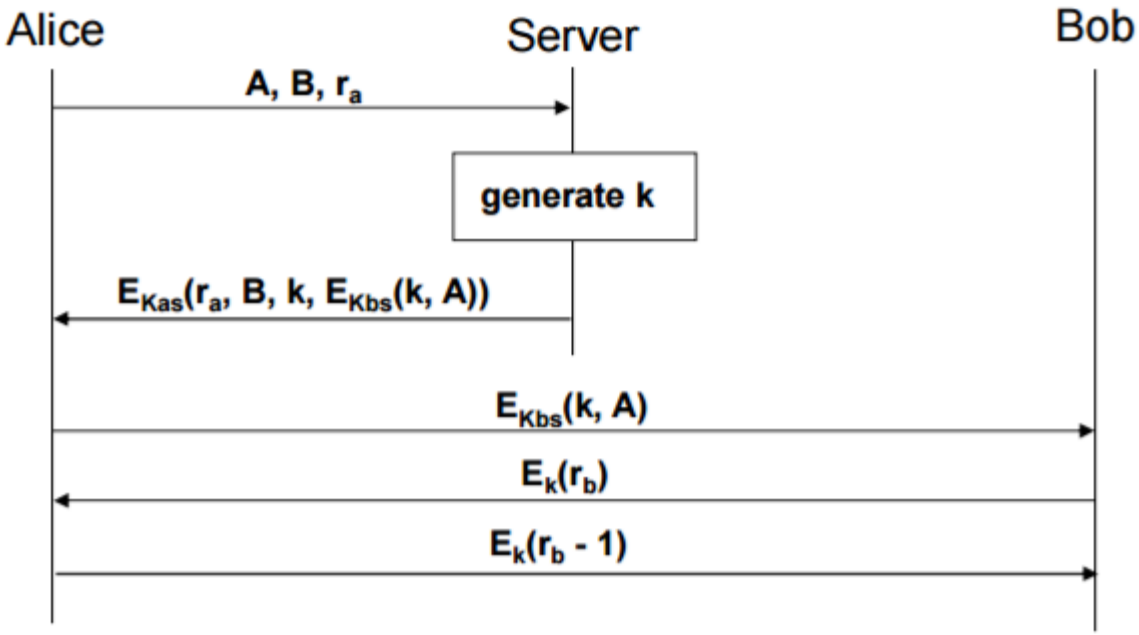


Probléma: nincs partnerhitelesítés

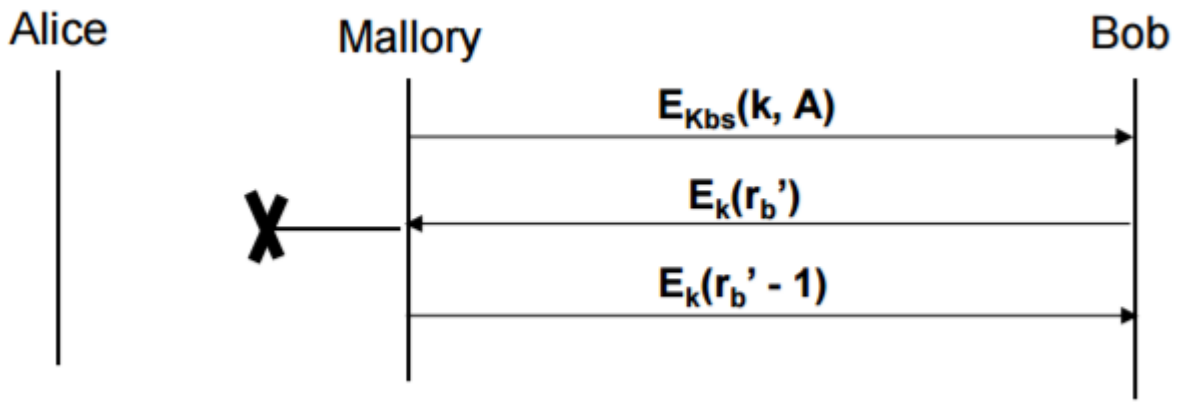
A Station-to-Station protokoll



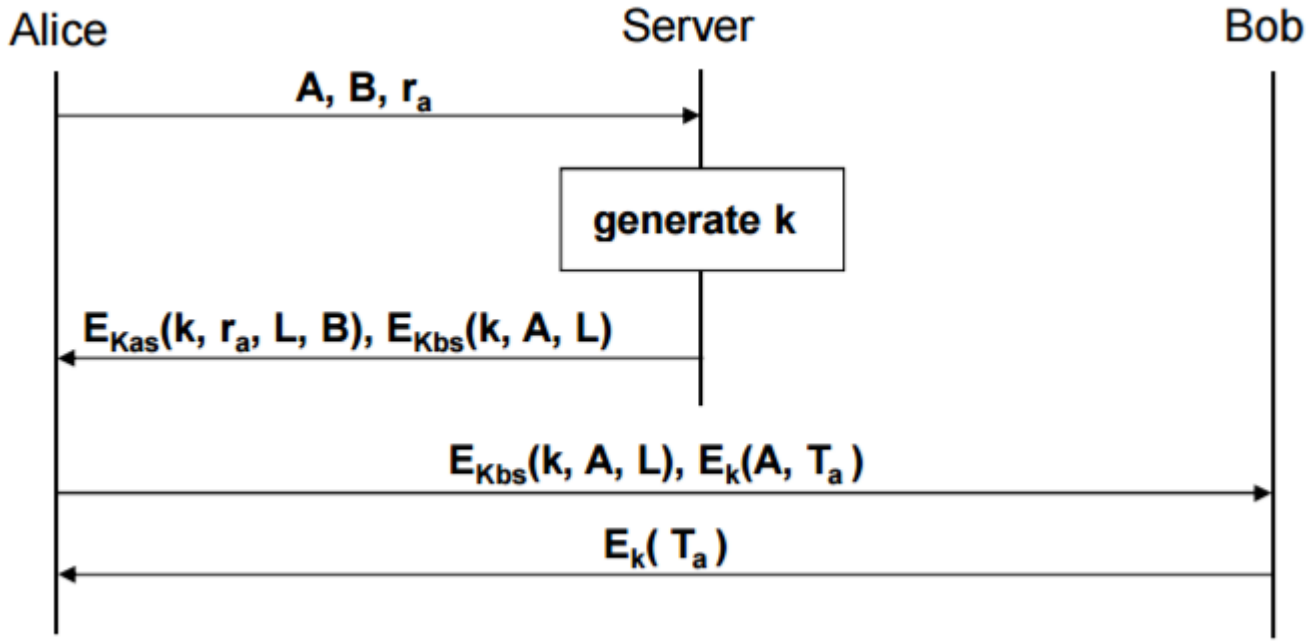
A Needham-Schroeder protokoll



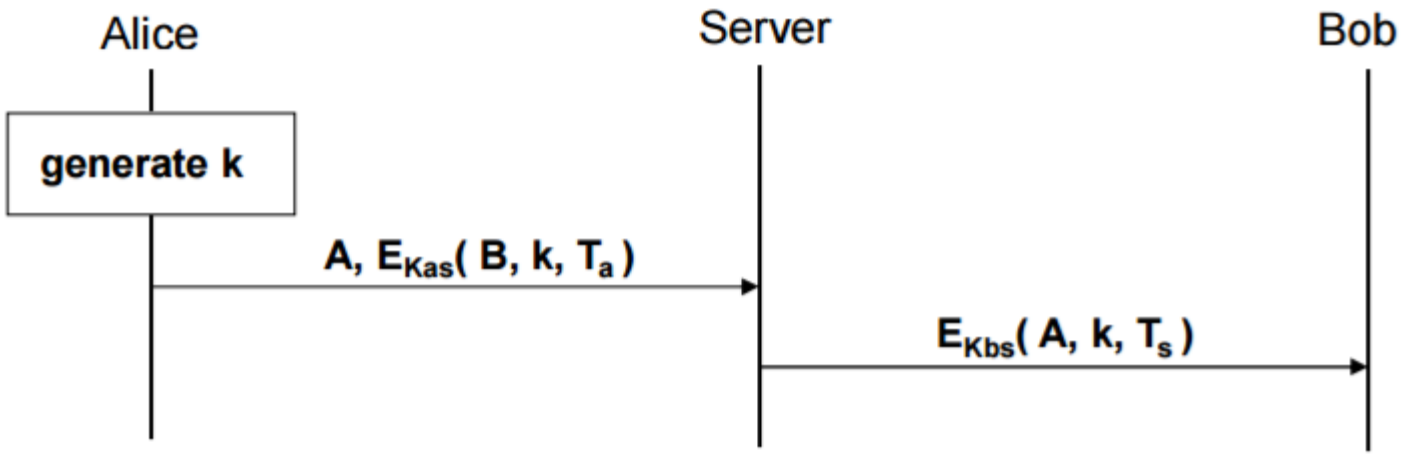
A Needham-Schroeder protokoll



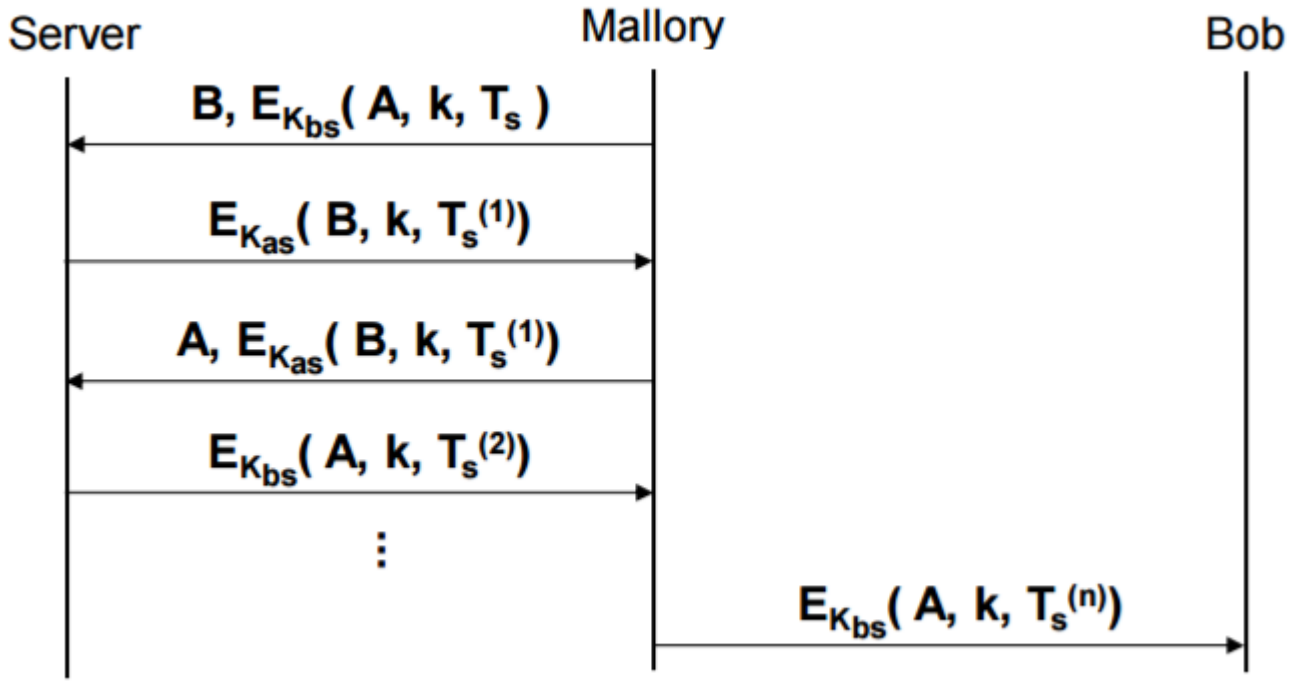
A Kerberos protokoll



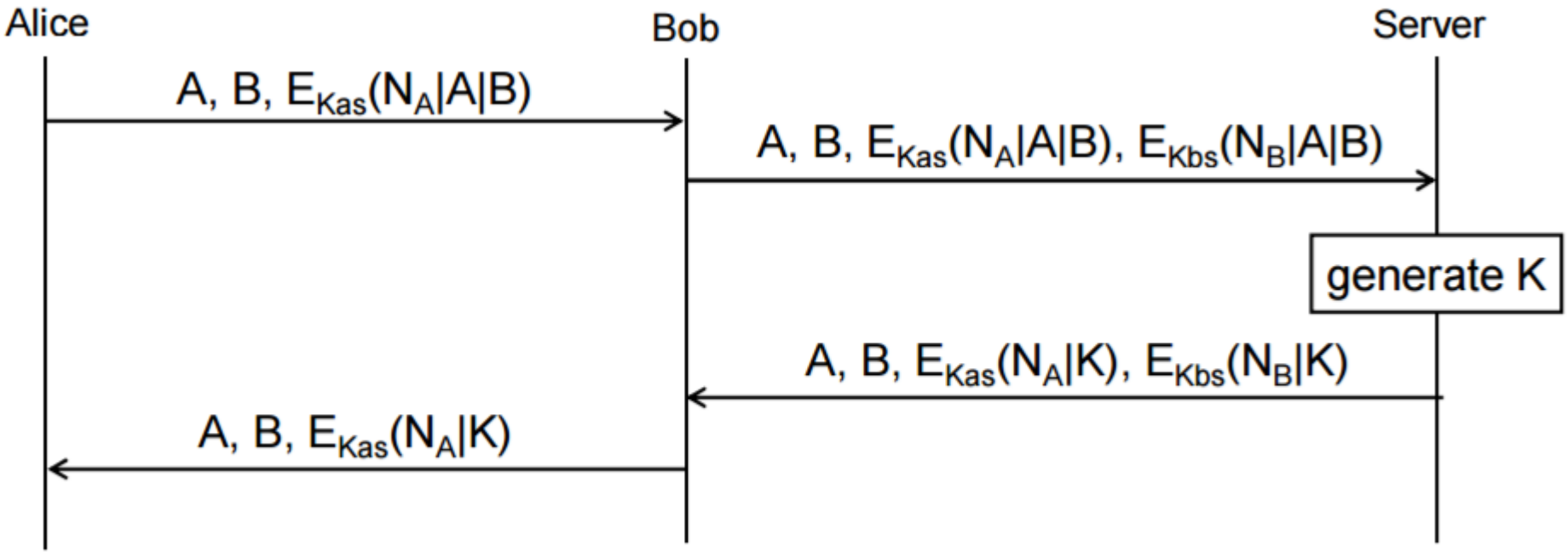
A Wide-Mouth-Frog protokoll



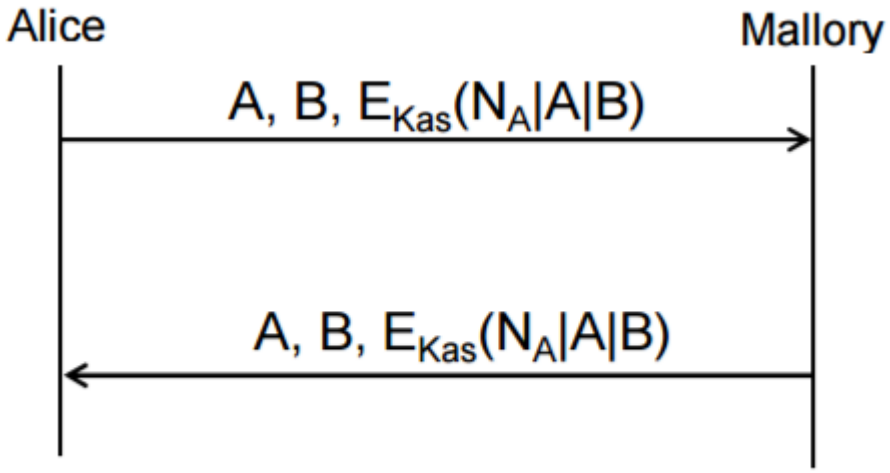
A Wide-Mouth-Frog protokoll



Az Otway-Rees protokoll



Az Otway-Rees protokoll



Köszönöm a figyelmet!