Óbudai Egyetem

Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

Műszaki területek informatikai biztonsága

Kulcscsere

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:

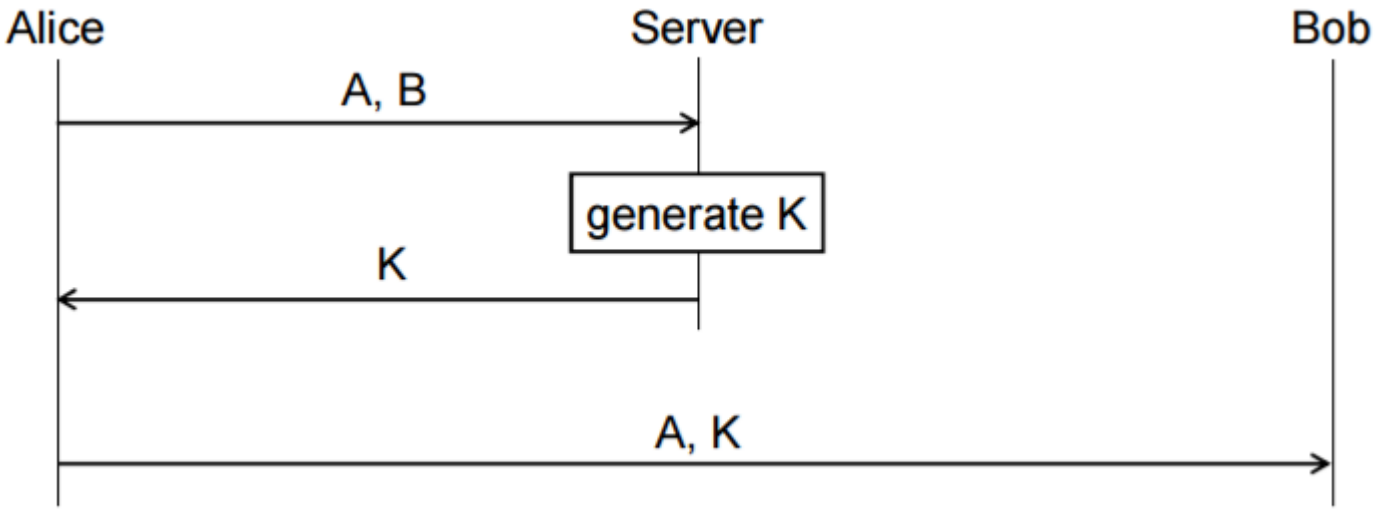
Kulcs transzport:

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

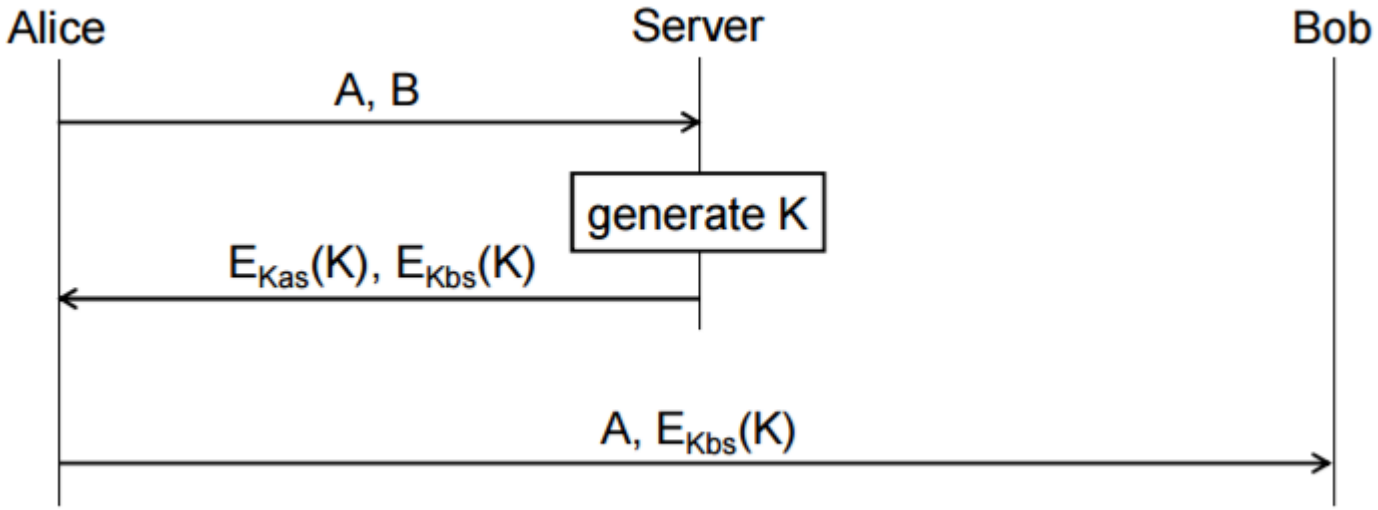
Kulcs megegyezés:

A kulcs a résztvevő felek által birtokolt információnak valamilyen együttes függvénye

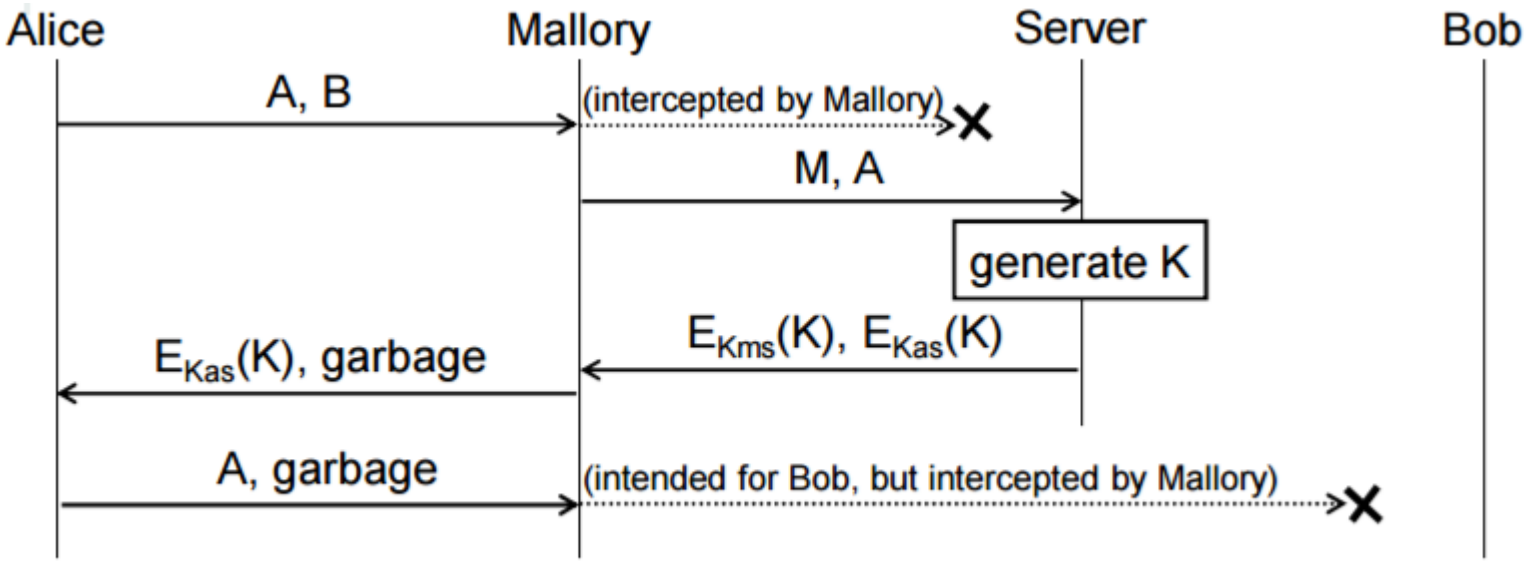
Kulcscsere protokollok



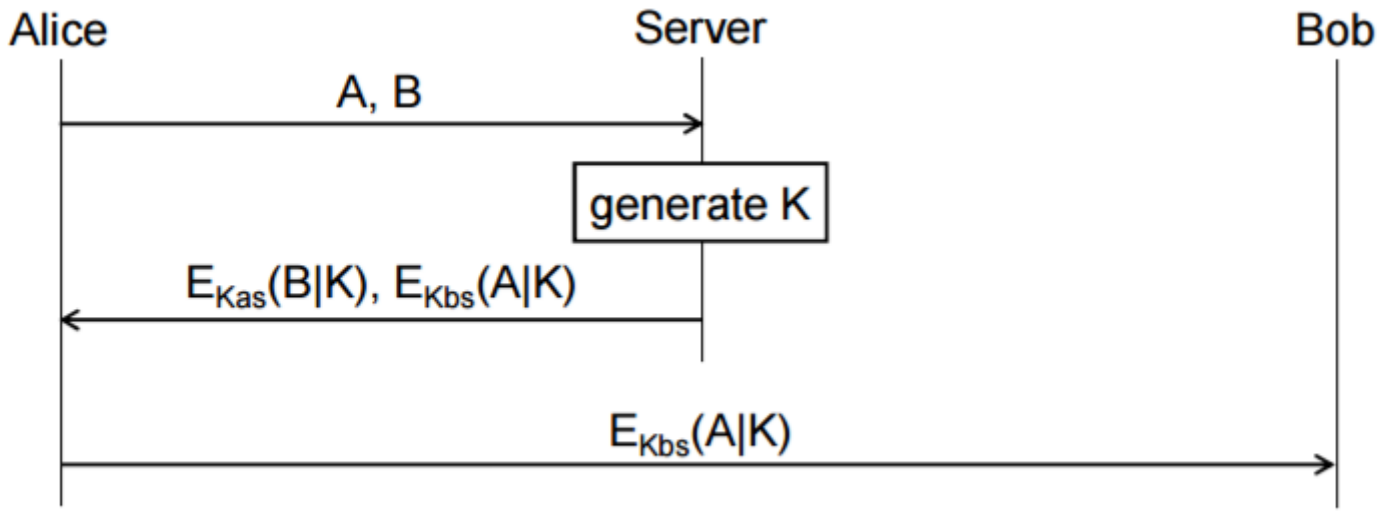
Kulcscsere protokollok



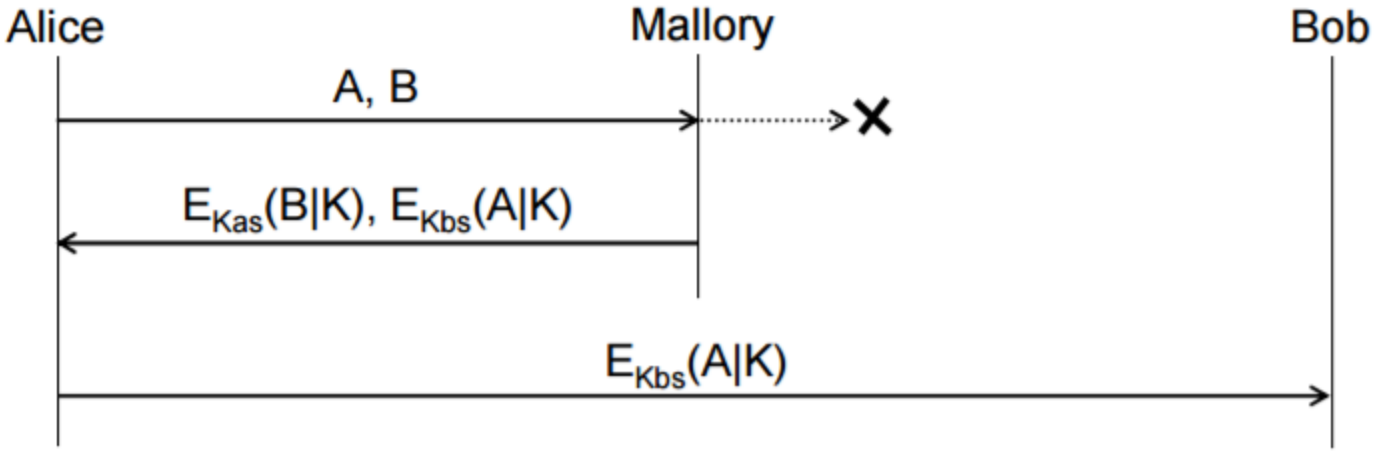
Kulcscsere protokollok



Kulcscsere protokollok



Kulcscsere protokollok



Kulcscsere protokollok

Hogyan garantáljuk a frissességet?

1) Időbélyeg:

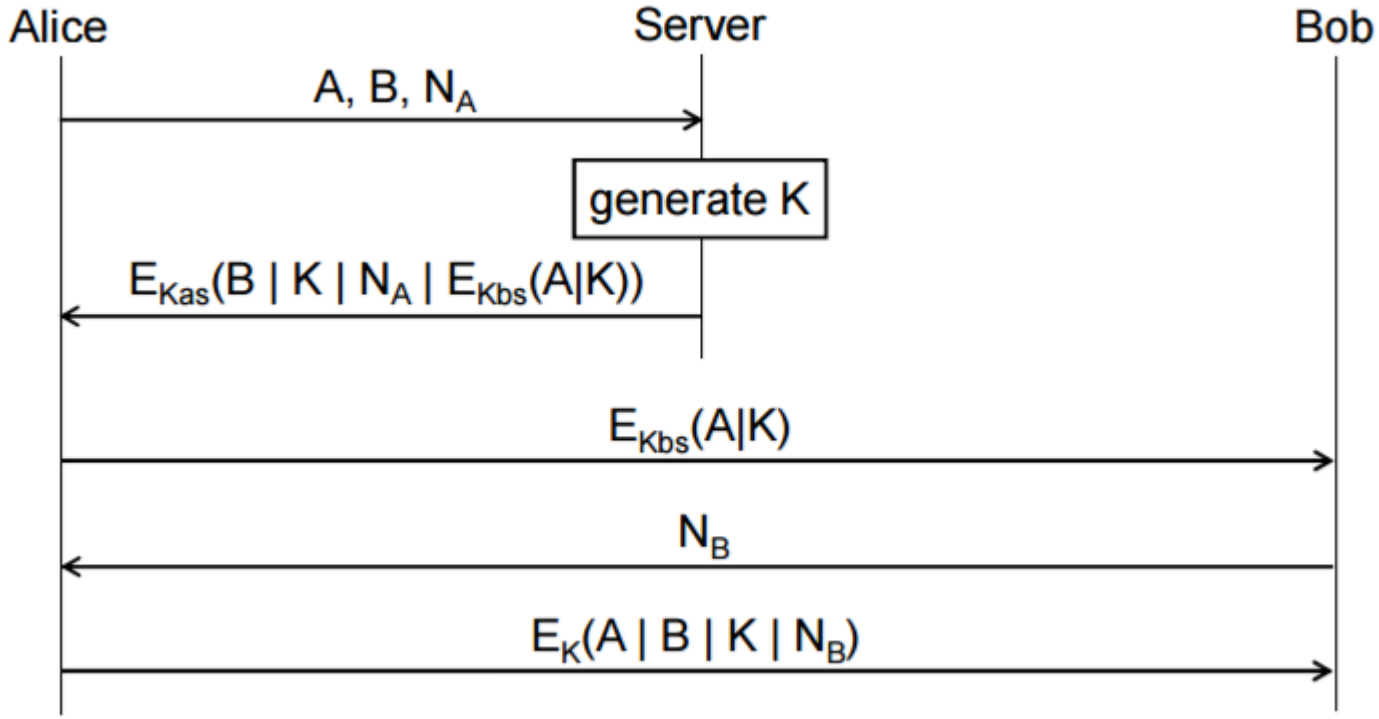
A szerver a kulcs generálásának idejét beágyazza az üzenetbe. Innentől számítva csak egy adott t időkorláton belül fogadható el a kulcs frissnek. Szinkronizáció szükséges.

2) Nonce:

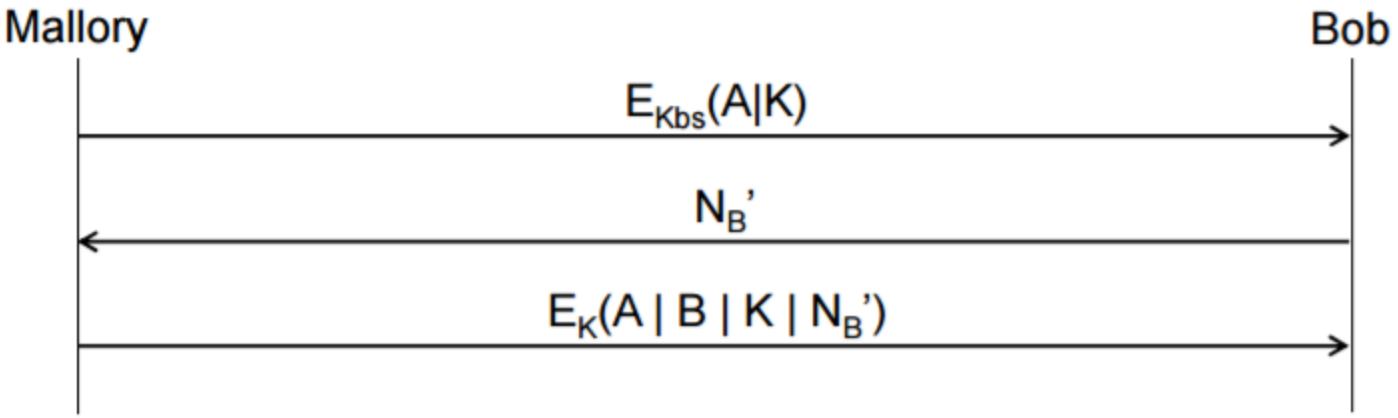
Valamely résztvevő generál egy véletlen számsorozatot, és ha a kulcscsere végén ez visszajut hozzá t időn belül, az bizonyítja számára a kulcs frissességét.

3) Kulcsmegegyezés

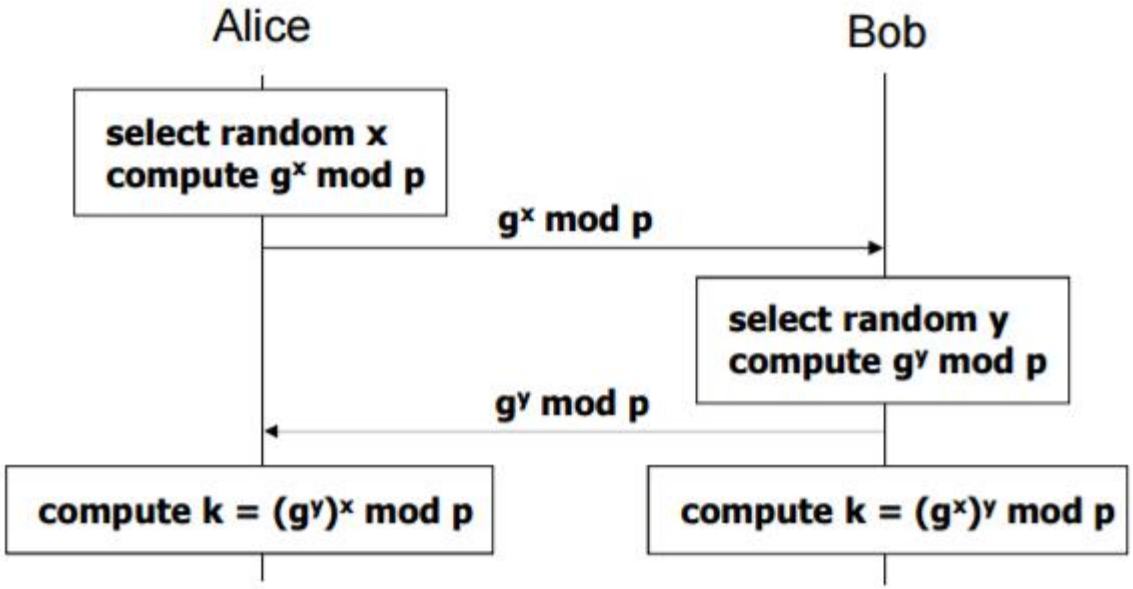
Kulcscsere protokollok



Kulcscsere protokollok



A Diffie-Hellman protokoll



Köszönöm a figyelmet!