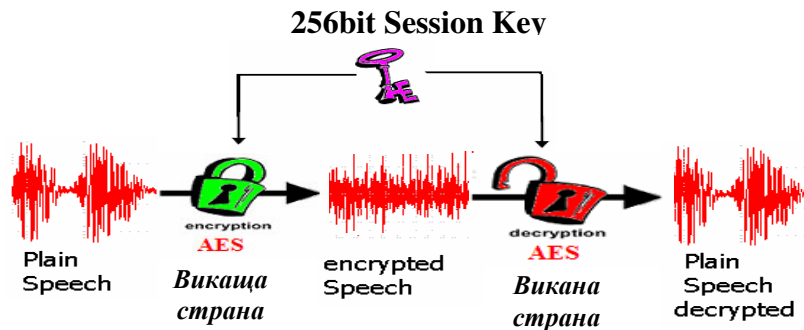


# Кое прави Enigma Ultra Secure GSM?



256bit сесийен ключ се предава от Викащата към Виканата страна под защитата на RSA крипто алгоритъм с 1024bit дължина на ключа.

Фиг. 1.0 Предаването на глас се криптира с AES крипто алгоритъм с 256bit сесийен ключ.

Основните стъпки за разбиване и подслушване на криптирането с Enigma са следните:

- 1) Достъп до **GSM air interface** или GSM мрежата и запис на потока от криптирани данни.
- 2) Извличане на **V110 data frames** от криптирания поток от данни, за да се отдели криптирания с **AES-256bit**, глас.
- 3) Декриптиране на криптирания с **AES-256bit**, глас, за да се извлече гласа кодиран в **AMBE –2000** формат.
- 4) Декодиране и **Playback AMBE** кодираната реч и подслушване на разговора.

Точки 1), 2) и 4) са изпълними с точното оборудване, технически познания и достъп.

Що се отнася до точка 3) – за да се декриптира AES-256bit криптираният поток от данни, трябва да са изпълнени успешно следните методи на атака:

- a) **Извличане на 256 bit Сесийен ключ използван за криптирането на конкретния разговор** - 256bit дължина на ключа представлява приблизително  $10^{77}$  възможни комбинации, което практически би отнело безкрайно дълго време за извличане на точния ключ.  
**Извод: Enigma издържа на атаки от тип a), така че атаки от следващо ниво биха могли да бъдат чрез метод b).**
- b) **Откриване на слабо място в алгоритъма AES** - AES е публичен алгоритъм, който е официално тестван и сертифициран от всички основни сертификационни служби.  
**Извод: Enigma издържа на атаки от тип b), така че атаки от следващо ниво биха могли да бъдат чрез метод c).**
- c) **Откриване на слабо място в криптирането чрез RSA 1024bit, за да се извлече Сесийният ключ, предаван по мрежата** - Преди обмяната на криптирани данни да започне, AES сесийният ключ се генерира и предава от викащата към виканата страна, по време на процеса на оторизация и размяна на ключове. Сесийният ключ се разменя в криптирана форма

като се използва RSA алгоритъм с RSA ключ с дължина 1024 bit. Така, че за да се извлече сесийният ключ, трябва да се разбие RSA-1024 bit-овото криптиране.

RSA е публичен алгоритъм и подобно на AES е сертифициран от съответните институции - напълно сигурен! RSA –1024 bit криптиране има приблизително  $10^{33}$  вероятни комбинации за ключа, поради което е безкрайно и достатъчно дълго времето за извличането му – практически невъзможно.

**Извод: Enigma издържа на атаки от тип c), така че атаки от следващо ниво биха могли да бъдат чрез метод d).**

**d) Извличане на Secret RSA ключ от Crypto картата** - По време на процеса на оторизация, сесийният ключ се генерира в Crypto картата, след което се криптира с RSA secret key в Crypto картата. Secret key никога не напуска сигурната среда на Crypto картата. Crypto картата е специално разработена с множество хардуерни и софтуерни механизми за защита срещу неоторизиран достъп до данните в нея. Crypto картата е официално тествана, одобрена и сертифицирана за ниво на защита E4+ за механична устойчивост съгласно ITSEC. Поради това е абсолютно невъзможно Secret key да бъде прочетен от нея.

**Извод: Enigma издържа на атаки от тип d), така че атаки от следващо ниво биха могли да бъдат чрез метод e).**

**e) Запазване и предоставяне на копие от RSA Key Pair от Telesec Trust Centre по време на издаването на Crypto картата** - Telesec Trust Centre работи съгласно и в съответствие със стриктното Германско (и Европейско) signature законодателство, според което Trust Centre е задължен да:

- Генерира уникална RSA двойка ключове за всяка Crypto карта и
- Да унищожава всички записи на RSA ключове след запис.

*Забележка:* За клиенти, които предпочитат да използват Enigma с RSA ключове генерирани от самите тях, ние можем да предложим допълнителен продукт (Customer CA) с който клиентите получават празни "Blank Crypto cards" и могат/трябва сами да записват свои RSA ключове.

**Извод: Enigma издържа на атаки от тип e), така че атаки от следващо ниво биха могли да бъдат чрез метод f).**

**f) Използване на откраднатата Enigma като част от „Middle Man attack“** - По време на всеки криптиран разговор, двата апарата взаимно правят проверки за оторизация, опознаване и идентификация. Това е възможно поради цифровият запис на всички RSA ключове от доверена трета страна. Защитени разговори могат да се правят само между два Enigma телефона, които имат Crypto карти издадени от Telesec Trust Centre или от клиента. При активиране на допълнителната функция „Затворена група абонати“ тази защита става още по-силна – разговори могат да се провеждат само между участниците в групата, още повече, изгубени телефони могат да се включат много лесно и бързо в т.нар. Black list. Това на практика категорично отстранява възможността за „middle man attack“.

**Извод: Enigma издържа на атаки от тип f), така че атаки от следващо ниво биха могли да бъдат чрез метод g).**

**g) Опит за разбиване на Enigma чрез Trojan software качен на апарата, с цел да се отслаби криптирането** - GSM апаратът и операционната система на неговият Security module имат функцията да отхвърлят неоторизирано download-ване на приложения от трета страна.

**Атаки от този тип са неприложими!**

**Системата Enigma предлага най-високото в момента ниво на защита на предаваните данни и глас!**