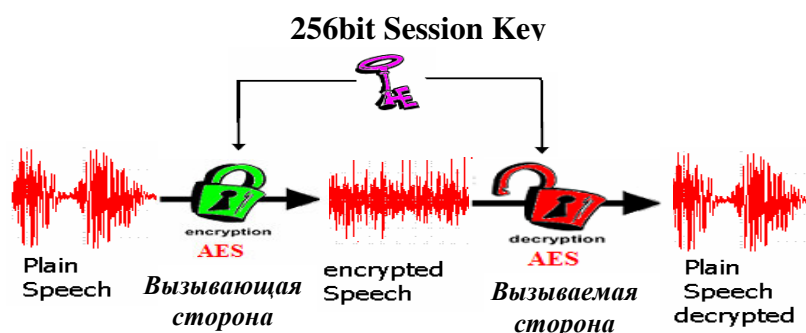


## Почему Enigma является Ultra Secure GSM?



сесийный ключ (256bit) передается с Вызывающей стороне к Вызываемой стороне, защищенным крипто алгоритма RSA 1024bit длина ключа.

Фиг. 1.0 Передача голоса шифруется крипто алгоритмом AES - 256bit

Основные способы применяющиеся для прослушивания сотовых крипто телефонов являются:

- 1) Доступа до GSM air interface или GSM сети и запись потока шифрованных данных.
- 2) Восстановление V110 data frames из зашифрованного потока данных, чтобы извлечь шифрованного AES-ом-256bit-ом голоса.
- 3) Дешифрование шифрованного AES-ом 256bit-ом голоса, чтобы восстановить кодированного AMBE-ом – 2000-ом формата голоса
- 4) Декодирование и Playback AMBE кодированного голоса и прослушивание разговора.

Пункты 1), 2) и 4) можно сделать пользуясь необходимым оборудованием, техническими познаниями и доступа.

Но в отношении пункта 3) – чтобы дешифровать шифрованном AES-256bit-ом поток данных, надо успешно выполнить следующие методы атаки:

**а) Восстановление 256 bit-ого сесийного ключа при помощи которого шифрован конкретный разговор.**

- 256bit-овая длина ключа представляет приблизительно  $10^{77}$  возможных комбинациях, которое практически заняло бы бескрайно длинное время для восстановления точного ключа.

*Вывод: Enigma устойчива атакой типа а), так что атаки на следующем уровне могли быть через применения метода б).*

**b) Открытие слабость алгоритма AES .**

- **AES** - это публичный алгоритм, официально испытан и сертифицирован всем основным сертификационным службам мира.

*Вывод: **Enigma** устойчива атакой типа **b)**, так что атаки на следующем уровне могли быть через применения метода **c)**.*

**c) Открытие слабость алгоритма RSA 1024bit, чтобы добиться сесийного ключа.**

Прежде чем начать обмена шифрованных данных, **AES**-ом генерируется сесийный ключ, который передается с вызывающей к вызываемой стороне во время проверки подлинности и обмена ключей. Сесийные ключи обмениваются в шифрованном виде пользуясь **RSA 1024 bit** алгоритма.

Так, что чтобы восстановить сесийного ключа надо взломать **RSA-1024 bit**-ового алгоритма. **RSA** - это публичный алгоритм и как **AES**-а, сертифицирован соответствующим службам - вполне безопасны!

У **RSA -1024 bit**-ового шифрования приблизительно  $10^{33}$  комбинациях ключа, для восстановления которого нужно очень длинное время - т.е. это практически невозможно.

*Вывод: **Enigma** устойчива атакой типа **c)**, так что атаки на следующем уровне могли быть через применения метода **d)**.*

**d) Извлечения **Secret RSA** ключа из **Crypto** карточке.**

Во время проверки подлинности, в **Crypto** карточке генерируется сесийный ключ, потом он шифруется **RSA secret key**-ом в **Crypto** карточке. **Secret key** никогда не покидает безопасной **Crypto** карточке. Она специально разработана с применением разнообразных аппаратных и программных механизмах для защиты против неотторизированного доступа до данные в нее.

**Crypto** карточка официально испытана, удобна и сертифицирована для степень защиты E4+ - механическая устойчивость согласно ITSEC. По этой причине, прочитать **Secret key**-я с карточкой, абсолютно невозможно.

*Вывод: **Enigma** устойчива атакой типа **d)**, так что атаки на следующем уровне могли быть через применения метода **e)**.*

**e) Сохранение и предоставление копию **RSA Key Pair**-а в **Telesec Trust Centre** во время создания **Crypto** карточкой.**

**Telesec Trust Centre** работает согласно и в соответствии со строгим Немецком (и Европейском) **signature** законодательством, в соответствии с которым **Trust Centre** обязан:

- а) Генерировать уникальная **RSA** пара ключей для каждой **Crypto** карточке, и
- б) Уничтожать все записи **RSA** ключей после записи.

Замечание: Клиенты, которые предпочитают пользоваться **Enigma**-ой с **RSA** ключами генерированы самим им, мы можем да предложим дополнительного продукта (Customer CA) при помощи которого клиенты получают «пустые» "Blank Crypto cards" и могут/надо сами записать своих RSA ключей.

*Вывод: **Enigma** устойчива атакой типа **e)**, так что атаки на следующем уровне могли быть через применения метода **f)**.*

**f) Применения украденной *Enigma*-ой как часть из „Middle Man attack“.**

Во время каждого зашифрованного разговора, оба аппарата делают взаимные проверки подлинности, ознакомление и идентификация.

Защищенные разговоры можно проводить только если у оба *Enigma* телефона *Crypto* карточки изданные *Telesec Trust Centre*-ом или клиентом.

Если применена дополнительная функция „Затворена группа абонентов“ эта защита становится еще сильнее – разговаривать могут только участники группой.

**Более того, потерянные телефоны можете включить легко и быстро в так называемом *Black list*.** Практически этим, категоричным образом устраняется возможность проведения „middle man attack“.

*Вывод: Enigma устойчива атакой типа f), так что атаки на следующем уровне могли быть через применения метода g).*

**g) Попытка подслушивания *Enigma*-ой через *Trojan software* в телефоне, с целью ослабление шифрования.**

У сотового телефона и операционной системе его *Security module* есть функция не позволяющая неотторизированного *download*-а.

*Вывод: Атаки и этого типа – неприложимые!*

Система *Enigma* предоставляет в данном моменте защита голоса и данных на самом высоком уровне.