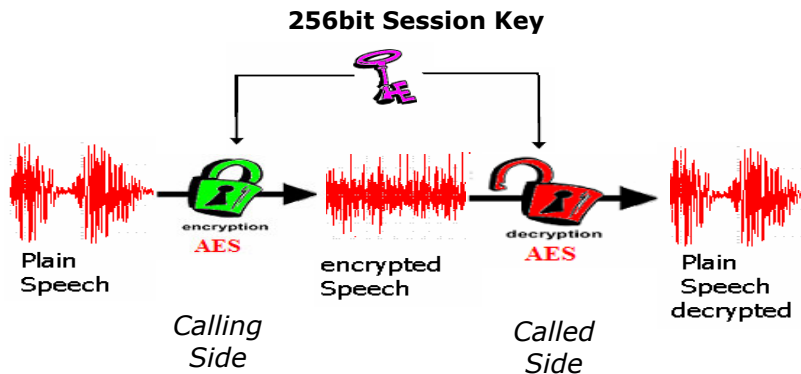


What Makes Enigma the Ultra Secure GSM Mobile?



256bit Session key passed from Calling side to Called side encrypted with RSA algorithm using 1024bit key length.

Figure 1.0 Enigma Speech is encrypted with AES algorithm using 256bit session key.

The Fundamental steps needed to listen in or break Enigma's encryption are as follows.

- 1st) Gain access to GSM air interface or GSM network and record the encrypted data stream.
- 2nd) From the recorded data stream, extract the V110 data frames to reveal the AES-256bit encrypted speech.
- 3rd) Decrypt AES-256bit encrypted speech to reveal speech data encoded to AMBE –2000 format.
- 4th) Decode and Playback AMBE encoded speech and listen to conversation.

Points 1), 2) and 4) are all possible with the right equipment, technical knowledge and access.

With Regard to point 3) to decrypt the AES-256bit encrypted speech requires any of the methods of attack listed below to be successful.

- a) **Deduce the 256 bit Session Key used to encrypt the speech** - 256bit key length represents approx 10^{77} possible key combinations and so it would take in all practical terms for eternity to deduce the right key.

Conclusion: Enigma is resistant to Attack by method a) so next attack level could be by method b).

- b) **Find a weakness in the AES algorithm** - AES algorithm is a public algorithm that has been formally tested and certified by all major governments to be cryptographically secure. No weakness exists.

Conclusion: Enigma is resistant to Attack by method b) so next attack level could be by method c)

- c) **Find a weakness in RSA 1024bit Encryption to extract Session Key that is sent over the air.** Prior to encrypted speech data is exchanged, the AES session key is generated and transmitted from calling side to called side during the exchanging keys phase of the secure call. The Session key is transmitted in encrypted format using RSA algorithm with RSA key length 1024 bit. So to extract the session key it is required to break RSA-1024 bit encryption. RSA algorithm is a public algorithm that has been formally tested and certified by all major governments to be cryptographically secure. No weakness exists for key length 1024 bits RSA –1024 bit encryption has approx 10^{33} possible key combinations and therefore so it would take in all practical terms for eternity to deduce the right key.

Conclusion: Enigma is resistant to Attack by method c) so next attack level could be by method d)



d) Extract the Secret RSA Key from the Crypto Card - During key exchange phase the Session key is generated inside the Crypto card and then encrypted with RSA secret key inside the Crypto card. The Secret key never leaves the secure environment of the Crypto card. The Crypto Card is a purpose developed smart card with multitude of hardware and Software security mechanisms to prevent unauthorised access to data secured in it. The Crypto Card has been formally tested and approved to be secure to E4+ mechanical strength high by ITSEC. So it is not possible for the Secret key to be read from the card.

Conclusion: Enigma is resistant to Attack by method d) so next attack level could be by method e)

e) Get a copy of the RSA Key Pair from Telesec Trust Centre during Crypto Card production -

The Telesec Trust Centre operates under strict German (and EU) signature law which dictates that the Trust Centre programming environment must a) Generate a unique RSA key pair for each Crypto Card and b) destroy all records of RSA keys after programming.

Note: For customers with requirements to operate Enigma with RSA keys generated by them then we have an optional product (Customer CA) which permits customer to receive "Blank Crypto cards" and to load their own RSA keys.

Conclusion: Enigma is resistant to Attack by method e) so next attack level could be by method f)

f) Use Stolen Enigma as part of an Middle Man attack - During every secure call the identify and authenticity of each Enigma unit is mutually checked. This is possible by digitally signing all RSA keys by a trusted Third party. This ensures that secure calls can only take place between two Enigma units which Contain Crypto Cards issued by either Telesec Trust Centre or by Customer own trust centre. With closed user group functionality this restriction is reduced further to ensure that secure calls can only take place between designated Enigma units within the closed group. Additionally lost Enigma units can be eliminated from a closed user group very easily and quickly. Thus Enigma eliminates the threat of middle man attack.

Conclusion: Enigma is resistant to Attack by method f) so next attack level could be by method g)

g) Try to Compromise the Enigma by loading Trojan software into it so that encryption is weakened or disabled - The GSM and Security module operating system has restricted functionality and security functions to prevent unauthorised download of third party applications.

Attack by point g) not feasible therefore;

In summary Enigma System offers highest level of protection for the voice data transmitted.