SIRAGA 331 - **modernste Chiffriertechnologie für die Sicherung Ihrer vertraulichen und geheimen Handy- Telefonate**

Mit den Siraga 331 – Crypto-Zusatzgeräten aller Modifikationen schuf

das Ingenieurbüro NachrichtenSicherheit Berlin,

eine andere Systemkomponente , welche Ihre Telefonate im sogenannten GSM-Funktelefonnetz (also mit allen „ normalen „ Funktelefonen) wirkungsvoll auf der Grundlage echter Zufallsfolgen und zuverlässig gegenüber allen unberechtigten Mithörversuchen sichert.
Der unberechtigte Angreifer hat keine Chanche , nur Ihr Gesprächspartner kann , geschützt vor fremden Ohren, Ihre Stimme hören . Genauso können nur Sie die Stimme Ihres Gesprächspartners verstehen.
Sehen Sie das grüne Signal oder im Display das Wort „ SICHER „, dann arbeitet Ihr hochsicherer Chiffrierkanal.

Die Verkehrsmethode ist eine individuelle, semiduplexe, Ende-zu-Ende Telefonie-Chiffrierverbindung, bei welcher nur die beiden Nutzer , Sie und Ihr Partner einen ca. 20 stelligen , mit einem echten Zufallsgenerator ermittelten Tagesschlüssel oder Sitzungsschlüssel kennen. Auf Wunsch werden Schlüsselunterlagen im Beisein der Nutzer erstellt.

Die Chiffriermethode ist die Blockchiffrierung durch Transposition. Zur unberechtigten Dechiffrierung durch jeden Angreifer müssen ca. 10^{200} Möglichkeiten der Zuordnung der einige ms -langen Sprachfetzen für jeden Block durchgerechnet werden. Selbst wenn die heutigen Computerkapazitäten mit 1000.000 multipliziert würden , würde es durchschnittlich Jahrhunderte dauern, um zum Klartext vorzudringen.

Das System :
Mit dem SIRAGA 331 können Sie mit allen SIRAGA 3.. Geräten Ihrer Gesprächspartner (SIRAGA - 31* für Festnetzverbindungen, - 32* für Internettelefonie über SKYPE u.ä. Systeme , - 33* für GSM- Funktelefone sowie SIRAGA – 34* für Satellitenverbindungen Verbindung aufnehmen und unabhängig vom Übertragungskanal zum Partner hochsichere Sprachver-bindungen betreiben , in denen Sie mit Ihrem Partner sicher und ohne unberechtigte Lauscher kommunizieren können.
Ist Ihr Gesprächspartner über ein analoges Funkgerät an das öffentliche Netz angeschaltet (z.B. über Überleiteinrichtungen / Seefunk) kann dieser mit Ihnen über SIRAGA 35* für analoge Funkgeräte sicher kommunizieren.

Die Benutzung :

Das Crypto- Zusatzgerät wird bei Bedarf angeschaltet. Es wird als separates Teil getragen und kann über eine integrierte Bluetooth- Einheit mit Ihrem Bluetooth – fähigen Handy gekoppelt werden.
Die Verbindung zum gewünschten Teilnehmer wird ganz normal mit dem offenen Handy hergestellt.
Wird eine verschlüsselte Verbindung gewünscht, stellen die Teilnehmer den entsprechenden Tages- oder Sitzungsschlüssel ein, schalten das Crypto – Zusatzgerät ein und telefonieren nun , nachdem sie sich überzeugt haben , daß die große grüne LED leuchtet , über die am Crypto – Zusatzgerät angeschaltete Sicherheits-Hör-Sprech- Garnitur.
Durch das Drücken der Sprechtaste wird der Sprechkanal geschaltet. Nach dem Loslassen hören Sie mit einer Verzögerung von ca. 3 Sekunden die entschlüsselte Sprache Ihres Partners.
Sie haben damit einen eigenen Telefonkanal , in den niemand eindringen kann, der nicht den Schlüssel besitzt.

SIRAGA 331 können Sie als SIRAGA 331 A in der Normalausführung mit Schlüsseleinstellmatrix oder als SIRAGA 331C , wie 331 A , jedoch mit garantierter Sicherheit, erwerben.