btt - Decypher

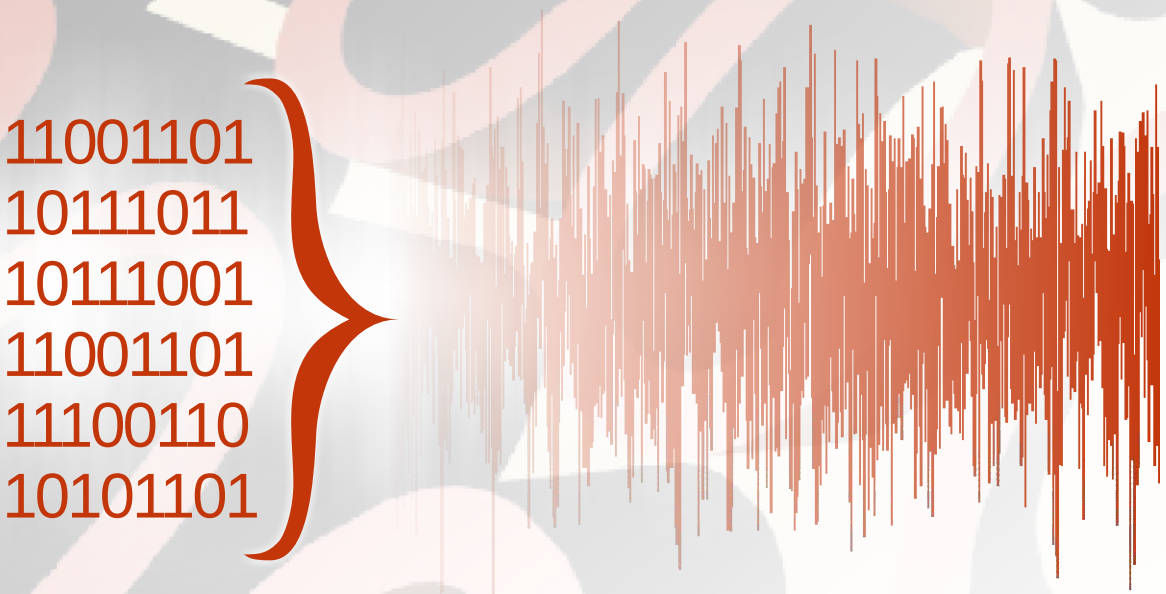
BTT Decipher provides A5/2 Decryption Algorithm.

The over-the-air privacy of GSM telephone conversations is protected by theA5 stream cipher. A5/2 version is used by 100s of millions customers in many countries, with A5/2 decoding product we supply a way to decipher A5/2 and extract the conversation key in less than a second.

Each GSM phone conversation can be encrypted by a new session key K,which is derived in a noninvertible way from the user's master key and a random value by another algorithm known as A8. By having some part of the traffic our A5/2 decoder is able to output the key.

Law enforcement agencies, public protection organisations that utilize GSM receiver can have A5/2 decypher unit to be incorporated into their receivers to enable them monitor the target phone conversation.

Customisation and development services are available upon request.



btt bilgi teknoloji tasarım ltd.
www.btt-int.com

btt - Decypher

Specifications:

Description and Capabilities:

The A52 decipher is expected to run as a single application on a Single Board Computer(S.B.C).

The A52 decipher board offers Kc extraction from SDCCH bursts.

Input to the extraction unit is 8 consecutive SDCCH/8 bursts or 12 consecutive SDCCH/4 bursts.

Output is 8 bytes of Kc.

Performance:

Current implementation is based on a Pentium-m processor, clocked at 1.8GHz with 2GBytes of RAM. Disk usage is 20GBytes;

Average response time is 25mSec. Max response time is 60mSec.

Minimum Requirements:

- Dedicated SBC
- 2 GBytes RAM
- 20 GBytes disk space
- Operating System Windows XP Pro SP2

Usage:

The board uses the GTCPLib communication library as an interface. The protocol is described using the C++ code below :

```
#define MSG_TYPE_DCU_KC 0x00000002
struct SDCUKey {DWORD MsgType; int Dmu; int SessionID; UINT64 Kc; DWORD TimeToFindKey; };
#define MSG_TYPE_DCU_BURSTS 0x00000003
struct SDCUBursts {DWORD MsgType; int Dmu; int SessionID; int NumBursts;
DWORD *FrameNumbers, BYTE *BurstData};
```