MysteryTwister

THE CRYPTO CHALLENGE CONTEST

PX-1000 Encryption (Part 1)

Author: Jörg Drobick

June 2024

History of the PX-1000

The PX-1000 was a small, portable message terminal with built-in encryption, which was developed by Text Lite in Amsterdam between 1980 and 1982. It was marketed as *Pocket Telex* (portable teletype-writer) and sold by Philips, among others. With the DES, the device offered secure encryption for the time.
In 1984, a new version called **PX-1000cr** was released, which used an alternative encryption algorithm developed by the NSA for this device.

Introduction to the PX-1000

The PX-1000 and the `cr` version were primarily designed for use by small companies and journalists, but were also used by the Dutch government.
It also played a role in the international fight for Nelson Mandela's release from prison. Some interesting background information on Operation Vula can be found at the Cryptomuseum [1].

The PX-1000 could be connected to a telephone in order to be able to send the messages entered. Messages were received in the same way and displayed on the device after decryption.
The original PX-1000 came onto the market in 1983. It could send messages of up to 7400 characters over a standard analog PSTN3 telephone line by holding the built-in acoustic modem on the back of the device to the microphone of the telephone handset.
Messages could then be received in the same way. The modem was held against the handset's loud-speaker to pick up the acoustic signals from the other end. To protect against eavesdropping, the device could encrypt messages using DES before transmission. DES was considered a very secure encryption algorithm at the time.

Further background information on the PX-1000 can also be found at cryptomuseum.com [2].
The history of the PX-1000 and the cryptography of the Cold War is placed in a larger context with current events in the work of J. R. Appelbaum. [3]

A back door?

However, the fact that the PX-1000 provided anyone with an extremely secure encryption algorithm greatly displeased the NSA. For this reason, the NSA contacted Philips' chief cryptologist at the time back in 1980 and asked for the DES to be replaced by the algorithm they had designed. Philips then approached TextLite and offered to reimburse them for all development costs plus compensation for discontinuing production. They also bought up all 10,000 devices already produced.

TextLite apparently could not refuse this offer, because only a few years later the new version of the PX-1000 appeared – without DES – but with the algorithm designed by the NSA.

How the PX-1000 works

To understand the structure of the ciphertext sent, consider the following example:
The plaintext used for encryption consists of 20 times `A`.
The key consists of 16 times `A`.

Header
The following header precedes the ciphertext: `0x01,0x80,0x18,0x4d`.

- `0x01` is the block number, it designates the first text block.
- `0x8018` is the indicator *ciphertext* + the length of the ciphertext without the 3 bytes checksum. In our example, the length is therefore 4 + 20 = 24 = `0x18`.
- `0x4d` stands for ciphertext, `0x48` is the indicator for “DUMP”.

Ciphertext

Block	Ciphertext	Checksum byte
Header	`0x01,0x80,0x18,0x4d`	-
1	`0x01,0xb5,0x7f,0xc3,0xf9,0x74,0xb8,0x3b`	`0x06`
2	`0x33,0xcc,0x66,0x5e,0xb1,0xf6,0x5e,0xf3`	`0x2d`
3	`0x72,0xca,0x7c,0x39,0x14,0xd2,0xd9,0xa6`	`0x44`

Checksum
The checksum is calculated by XORing all 8 bytes of the ciphertext block.

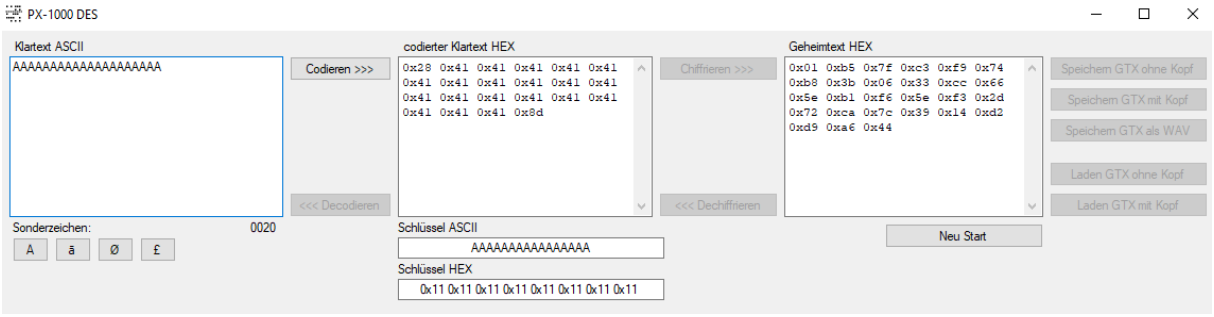
Encryption
Together with the header (4 bytes) and the three checksum bytes (3 bytes), the ciphertext is 27 bytes long.

In some implementations, the byte `0x28` is inserted directly after the header to mark the start of the ciphertext. Equivalently, the byte `0x8d` is inserted at the end of the ciphertext. Both bytes are encrypted along and are removed after decryption.

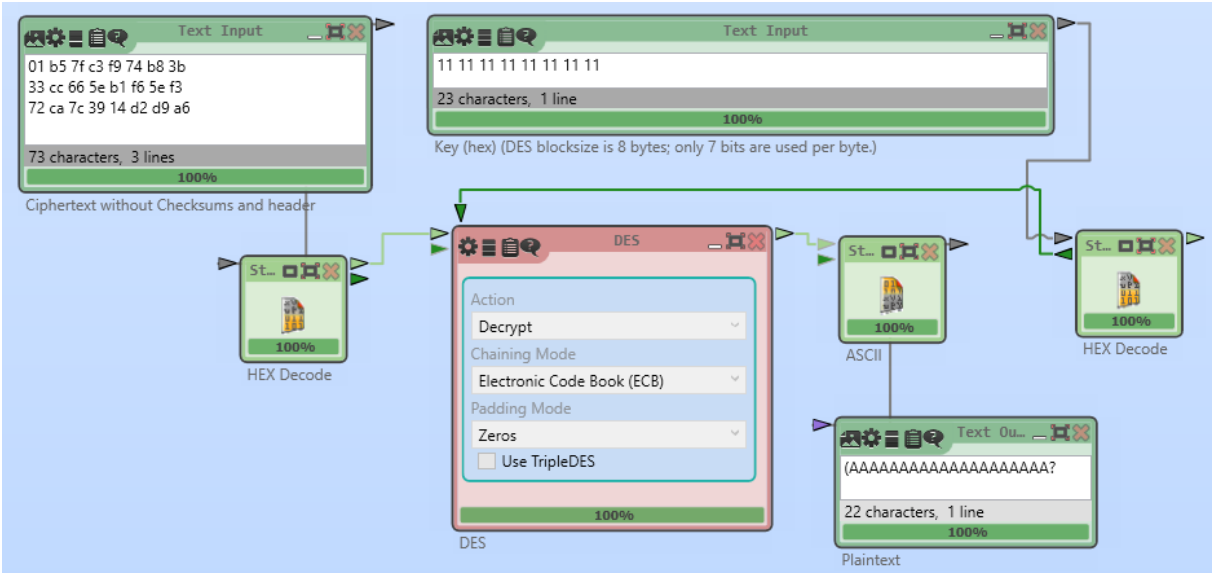
For encryption and decryption, DES is used with ECB (Electronic Code Book Mode).
As DES was used in ECB mode, identical plaintext blocks are encrypted to identical ciphertext blocks.
After removing the checksum bytes, the header and, if necessary, the start and end bytes, the ciphertexts can be decrypted.
The key used in this example is: `AAAAAAAAAAAAAAAAA`, which is converted by the PX-1000 into `0x11,0x11,0x11,0x11,0x11,0x11,0x11,0x11`.

Software

A tool for understanding the PX-1000 and decrypting the ciphertext is available from the author. [4]



Alternatively, CrypTool 2 can also be used [5].
Header and checksum bytes must first be removed, and the key has to be converted.



The Challenge

This challenge is about decrypting a text that has been encrypted with a PX-1000 (DES, ECB). The ciphertext is available as a file (`PX1000.pxc`) including all headers, just as the data would have been

transmitted through the modem of a PX-1000 and would have been *interceptable*.
The challenge is part one in three challenges about the PX-1000. In the second part we look at the `cr` version of the challenge, i.e. the version modified by the NSA. The third part deals with the `TC850`, a similarly functioning encryption device from the Swiss company GRETAG.

For decryption, the author provides a collection of tools and information on the PX-1000. Among other things, a complete explanation of how the PX-1000 encryption and transmission works, as well as reverse-engineered emulators of the PX-1000 and PX-1000cr verified against the originals. [6]

First, the structure of the ciphertext must be analyzed.

The key derivation is to be reproduced using the tool created by the author [4].

The solution is the decrypted plaintext.

- Upper and lower case letters and punctuation marks must be retained.
- The key consists of two concatenated English words.

Additional files

- `PX1000.pxc` - Ciphertext with all headers (binary file)

References

[1] cryptomuseum.com: Exciting details about operation vula
[2] cryptomuseum.com: Background information on the PX-1000
[3] Appelbaum, J. R.: Communication in a world of pervasive surveillance (2022)
[4] Drobick, J.: PX-1000 tool (windows)
[5] CrypTool 2 download (windows) *CrypTool Contributors*
[6] Drobick, J.: Author's website about the PX-1000 (german)