On the insecurity of interchanged use of OFB and CBC modes of operation

Danilo Gligoroski

Centre for Quantifiable Quality of Service in Communication Systems, Norwegian University of Science and Technology, O.S.Bragstads plass 2E, N-7491 Trondheim, NORWAY
danilo.gligoroski@q2s.ntnu.no

Abstract. The security of interchanged use of modes of operation of block ciphers have not been discussed in the public literature. So far, the modes of operation of block ciphers have been treated as completely independent and uncorrelated. In this paper we represent both CBC and OFB as quasigroup string transformations, and then show that OFB mode is a special case of the CBC mode of operation. That raise possibilities for construction of several devastating attack scenarios against that interchanged use of CBC and OFB. These attacks have not been addressed in NIST Special Publication 800-38A 2001, "Recommendation for Block Cipher Modes of Operation". More specifically, in the chosen plaintext attack scenario with interchanged use of CBC and OFB mode, we give a concrete list of openssl commands that extract the complete plaintext without knowing the secret key.

Key words: *block ciphers, modes of operation, quasigroup string transformations*

1 Introduction

The first standardized approach to modes of operation for block ciphers was introduced in 1980 by NIST (in that time National Bureau of Standards) for the block cipher DES [10]. Then, at the end of the AES competition process, NIST organized two workshops for modes of operation of block ciphers [11]. Several new modes of operation have been proposed such as Accumulated Block Chaining (ABC) of Knudsen [8], Rogaway's Parallelizable Authenticated Encryption (OCB) [14], Key Feedback Mode was proposed by Håstad and Näslund [6], Gligor and Donescu proposed eXtended Ciphertext Block Chaining (XCBC) schemes [5] and Jutla proposed a parallelizable encryption mode with message integrity [7]. As a result of those workshops and the suggestions given by numerous cryptographers and other experts in the field, NIST compiled a Special Publication 800-38A 2001 (SP800-38A), "Recommendation for Block Cipher Modes of Operation" [12]. In that document five modes of operation are fully specified and recommend. Those modes of operation are: Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), and Counter (CTR). While, the particular use and the security concerns of all those modes are discussed in that document, there is nothing about the security concerns when those modes are used interchangeably. For example, it is well known fact that the keystream reuse is insecure, and it is well elaborated at several places in the NIST document SP800-38A, where the recommendations how to choose IVs are given. However, it is perfectly possible to use the keystream produced in one mode of operation for the first time, but the same keystream in a form of a ciphertext to be produced by other mode too. So, formally speaking, the request for not reusing the keystreams for a particular mode can be obeyed, but still that keystream can be produced by other mode of operation, thus causing the whole plaintext to be completely disclosed.

Of coarse, it is natural to rise the question: "Is the interchange use of several modes of operation possible in practice?" We think that it is possible. Namely, very often software packets or libraries are offering a set of block ciphers together with all five NIST modes of operation (see for example OpenSSL [13] or Crypto++ [2] - to name a few).

Our results

In this paper we will show that, both CBC and OFB modes of operations can be defined as a quasigroup string transformations. From that perspective, we will show that OFB mode is a special case of the more general mode CBC. Then, by using the freedom of choice within the software packages that offer both CBC and OFB modes of operation and still fully complying with the NIST recommendations, we will show how someone can successfully extract the plaintext from the ciphertext, without the knowledge of the secret key.

The organization of the paper is following: In section 2 we give short introduction, basic definitions and properties of quasigroup string transformations, CBC and OFB modes of operation and represent those modes as quasigroup string transformations. In section 3 we describe several attack scenarios that extracts complete plaintext without knowledge of the secret key. There we give an example with a concrete list of openssl commands that will show the insecurity of the combination of OFB and CBC mode. In section 4 we give conclusions.

2 Basic definitions

2.1 Quasigroup string transformations

Here we give just a few definitions about quasigroups and quasigroup string transformations. A more detailed explanation is found in [1, 3, 9, 15].

Definition 1. *A quasigroup $(Q, *)$ is a groupoid satisfying the law*

$$(\forall u, v \in Q)(\exists! x, y \in Q) \quad u * x = v \ \& \ y * u = v. \tag{1}$$

It follows from (1) that for each $a, b \in Q$ there is a unique $x \in Q$ such that $a * x = b$. Then we denote $x = a \setminus_* b$ where $\setminus_*$ is a binary operation in Q (called a left parastrophe or left conjugate of $*$) and the groupoid $(Q, \setminus_*)$ is a quasigroup too. The algebra $(Q, *, \setminus_*)$ satisfies the identities

$$x \setminus_* (x * y) = y, \quad x * (x \setminus_* y) = y. \tag{2}$$

Consider an alphabet (i.e., a finite set) Q, and denote by Q^+ the set of all nonempty words (i.e., finite strings) formed by the elements of Q. In this paper, depending on the context, we will use two notifications for the elements of Q^+: $a_1 a_2 \dots a_n$ and $(a_1, a_2, \dots, a_n)$, where $a_i \in Q$. Let $*$ be a quasigroup operation on the set Q. For each $l \in Q$ we define two functions $e_{l,*}, d_{l,*} : Q^+ \longrightarrow Q^+$ as follows:

Definition 2. *Let $a_i \in Q$, $M = a_1 a_2 \dots a_n$. Then*

$$e_{l,*}(M) = b_1 b_2 \dots b_n \iff b_1 = l * a_1,\ b_2 = b_1 * a_2, \dots,\ b_n = b_{n-1} * a_n,$$

$$d_{l,*}(M) = c_1 c_2 \dots c_n \iff c_1 = l * a_1,\ c_2 = a_1 * a_2, \dots,\ c_n = a_{n-1} * a_n,$$

i.e., $b_{i+1} = b_i * a_{i+1}$ and $c_{i+1} = a_i * a_{i+1}$ for each $i = 0, 1, \dots, n-1$, where $b_0 = a_0 = l$.

The functions $e_{l,*}$ and $d_{l,*}$ are called the e–transformation and the d–transformation of Q^+ based on the operation $*$ with leader l respectively, and their graphical representations are shown in Fig. 1.

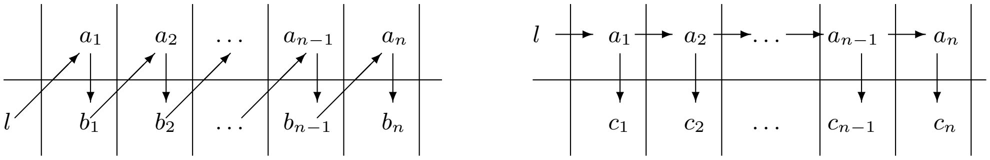


Fig. 1. Graphical representations of the $e_{l,*}$ and $d_{l,*}$ transformations

By straightforward application of the Definition 2 and the identities (2) it is easy to prove the following:

Theorem 1. *If $(Q, *)$ is a finite quasigroup, then $e_{l,*}$ and $d_{l,\backslash_*}$ are mutually inverse permutations of Q^+, i.e.,*

$$d_{l,\backslash_*}(e_{l,*}(M)) = M = e_{l,*}(d_{l,\backslash_*}(M))$$

for each leader $l \in Q$ and for every string $M \in Q^+$. □

2.2 CBC and OFB mode of operation as quasigroup string transformations

We will use the same terminology and notation as it is defined in SP800-38A [12].

- The forward cipher function of the block cipher algorithm under the key K applied to the data block X is denoted as $CIPH_K(X)$.
- The inverse cipher function of the block cipher algorithm under the key K applied to the data block X is denoted as $CIPH_K^{-1}(X)$.
- The bitwise exclusive-OR of two bit strings X and Y of the same length is denoted as $X \oplus Y$.
- The plaintext will be denoted as a sequence of n blocks $P = P_1, P_2, \dots, P_{n-1}, P_n$ where every P_i has the length in bits that is characteristic for the particular block cipher.
- The ciphertext will be denoted as a sequence of n blocks $C = C_1, C_2, \dots, C_{n-1}, C_n$ where every C_i has the length in bits that is also characteristic for the particular block cipher.
- The block size in bits is characteristic for the particular block cipher and will be denoted with b. (For AES $b = 128$.)
- The key size in bits will be denoted with k. (For AES $k = 128, 192, 256$.)
- The string consisting only of zero bits will be denoted as $\mathbf{0}$.

For some of the modes of operation, the last plaintext block P_n or the last ciphertext block C_n are allowed to have less bits than the block size, and in the NIST publication they are denoted as P_n^* and C_n^*. Without the loss of generality concerning the security issues, throughout this paper we will take that the last parts of the plaintext and ciphertext have also the length of the block size.

According to SP800-38A, *The Cipher Block Chaining (CBC) mode is a confidentiality mode whose encryption process features the combining (chaining) of the plaintext blocks with the previous ciphertext blocks. The CBC mode requires an IV to combine with the first plaintext block. The IV need not be secret, but it must be unpredictable. Also, the integrity of the IV should be protected.* The CBC mode is defined as follows:

$$\textbf{CBC Encryption:} \qquad C_j = CIPH_K(C_{j-1} \oplus P_j), \quad j = 1, \ldots, n$$

$$\textbf{CBC Decryption:} \qquad P_j = CIPH_K^{-1}(C_j) \oplus C_{j-1}, \quad j = 1, \ldots, n$$

where $C_0 = IV$ is so called *Initial Value.*

Definition 3. *For every $A, B \in \{0,1\}^b$, and every key $K \in \{0,1\}^k$ let us define the following operation:*

$$A * B \equiv CIPH_K(A \oplus B).$$

Theorem 2. *The operation $*$ is a commutative quasigroup operation in the set $\{0,1\}^b$.*

Proof. The commutativity of the operation $*$ follows immediately from the commutativity of the operation $\oplus$. Namely, for any chosen key K it is true that

$$A * B = CIPH_K(A \oplus B) = CIPH_K(B \oplus A) = B * A.$$

Now to proof that the operation $*$ is a quasigroup operation it is sufficient to prove that the equation $A * X = B$ has unique solution, for any $A, B \in \{0,1\}^b$. And since the block cipher $CIPH_K(\cdot)$ is a bijection in $\{0,1\}^b$ the equation $A * X = B$ has a unique solution $X = CIPH_K^{-1}(B) \oplus A$. □

Proposition 1. *The left parastrophe operation $\backslash_*$ that is corresponding to the operation $*$ is:*

$$A \backslash_* B \equiv CIPH^{-1}(B) \oplus A.$$

Proof. We have to prove that identities (2) are satisfied. First,

$$A \backslash_* (A * B) = CIPH_K^{-1}(A * B) \oplus A = CIPH_K^{-1}(CIPH_K(A \oplus B)) \oplus A = (A \oplus B) \oplus A = B,$$

and then

$$A * (A \backslash_* B) = A * (CIPH_K^{-1}(B) \oplus A) = CIPH_K(A \oplus (CIPH_K^{-1}(B) \oplus A)) = CIPH_K(CIPH^{-1}(B)) = B.$$

□

Theorem 3. *The CBC mode of operation is equivalent with the following quasigroup string transformations:*

$$\textbf{CBC Encryption:} \qquad C = e_{IV,*}(P_1, P_2, \ldots, P_n),$$

$$\textbf{CBC Decryption:} \qquad P = d_{IV,\backslash_*}(C_1, C_2, \ldots, C_n),$$

Proof. If we apply directly the Definition 2, of e–transformation and d–transformation with a leader IV we will obtain the corresponding values of the ciphertext C and the plaintext P. □

According to SP800-38A, *The Output Feedback (OFB) mode is a confidentiality mode that features the iteration of the forward cipher on an IV to generate a sequence of output blocks that are exclusive-ORed with the plaintext to produce the ciphertext, and vice versa. The OFB mode requires that the IV is a nonce, i.e., the IV must be unique for each execution of the mode under the given key.* The OFB mode is defined as follows (supposing that the plaintext has length that is multiple of the block size):

$$\begin{array}{lll} \textbf{OFB Encryption:} & I_1 = IV; & \\ & I_j = O_{j-1}, & \text{for } \ j = 2, \ldots, n; \\ & O_j = CIPH_K(I_j), & \text{for } \ j = 1, \ldots, n; \\ & C_j = P_j \oplus O_j, & \text{for } \ j = 1, \ldots, n; \end{array}$$

$$\begin{array}{lll} \textbf{OFB Decryption:} & I_1 = IV; & \\ & I_j = O_{j-1}, & \text{for } \ j = 2, \ldots, n; \\ & O_j = CIPH_K(I_j), & \text{for } \ j = 1, \ldots, n; \\ & P_j = C_j \oplus O_j, & \text{for } \ j = 1, \ldots, n; \end{array}$$

Further in the text we will use the notation $C_{OFB} = OFB_{K,IV,encrypt}(P)$ as a short notation for OFB encryption of a plaintext P with a key K and an initial value IV.

Theorem 4. *The OFB mode of operation is equivalent with the following quasigroup string transformations:*

$$\textbf{OFB Encryption:} \qquad C = e_{IV,*}(\mathbf{0}) \oplus P,$$

$$\textbf{OFB Decryption:} \qquad P = e_{IV,*}(\mathbf{0}) \oplus C,$$

Proof. If we apply directly the Definition 2, of e–transformation on the string **0** with a leader IV we will obtain the corresponding values of the ciphertext C and the plaintext P. □

From the last Theorem it is clear that the OFB mode is a special case of the CBC mode of operation where the zero string **0** is encrypted. That raise possibilities to define several attacks with chosen plaintext, that employ interchanged use of CBC and OFB mode of operation. Those attacks are described in the next section.

3 Scenarios of attacks with chosen plaintext on the interchanged use of CBC and OFB mode of operation

From all definitions, properties and theorems in the previous section it is clear that the following Theorem is true:

Theorem 5. *Let $K \in \{0,1\}^k$ be a secret key and let $IV \in \{0,1\}^b$ be an initial value. Let $C_{CBC} = e_{IV,*}(\mathbf{0})$ is a cipher text obtained by the encryption of the plaintext $P_{CBC} = \mathbf{0}$ in the CBC mode of encryption, with the secret key K and initial value IV. Then, any ciphertext C_{OFB} obtained by the OFB mode of operation with a secret key K and the initial value IV that is the same as in the CBC mode (and is also nonce for the OFB mode) can be decrypted simply by the operation*

$$P = C_{CBC} \oplus C_{OFB}.$$

□

In this section we will discuss three variants of a known plaintext attack, where interchanged use of CBC and OFB modes of operation are performed, and where requirements of the NIST recommendations are fulfilled.

Attack 1 is just step by step description of the Theorem 5.

Attack 1.

Step 1. The attacker Eve knows the encryption of the string $\mathbf{0}$ i.e. she knows $C_{CBC} = e_{IV_{CBC},*}(\mathbf{0})$. She also knows the initial value IV_{CBC} for that encryption, but does not know the secret key K.

Step 2. Alice and Bob possess the secret key K, and decide to perform a secure communication using the OFB mode.

Step 3. In the NIST recommendations for IV in OFB mode (page 13 of [12]) it is written that *"The OFB mode requires that the IV is a nonce, i.e., the IV must be unique for each execution of the mode under the given key;"* According to those recommendations, the use of IV_{CBC} is allowed since it has never been used in OFB mode.

Step 4. Alice encrypts the plaintext P performing $C_{OFB} = OFB_{K,IV_{CBC},encrypt}(P)$.

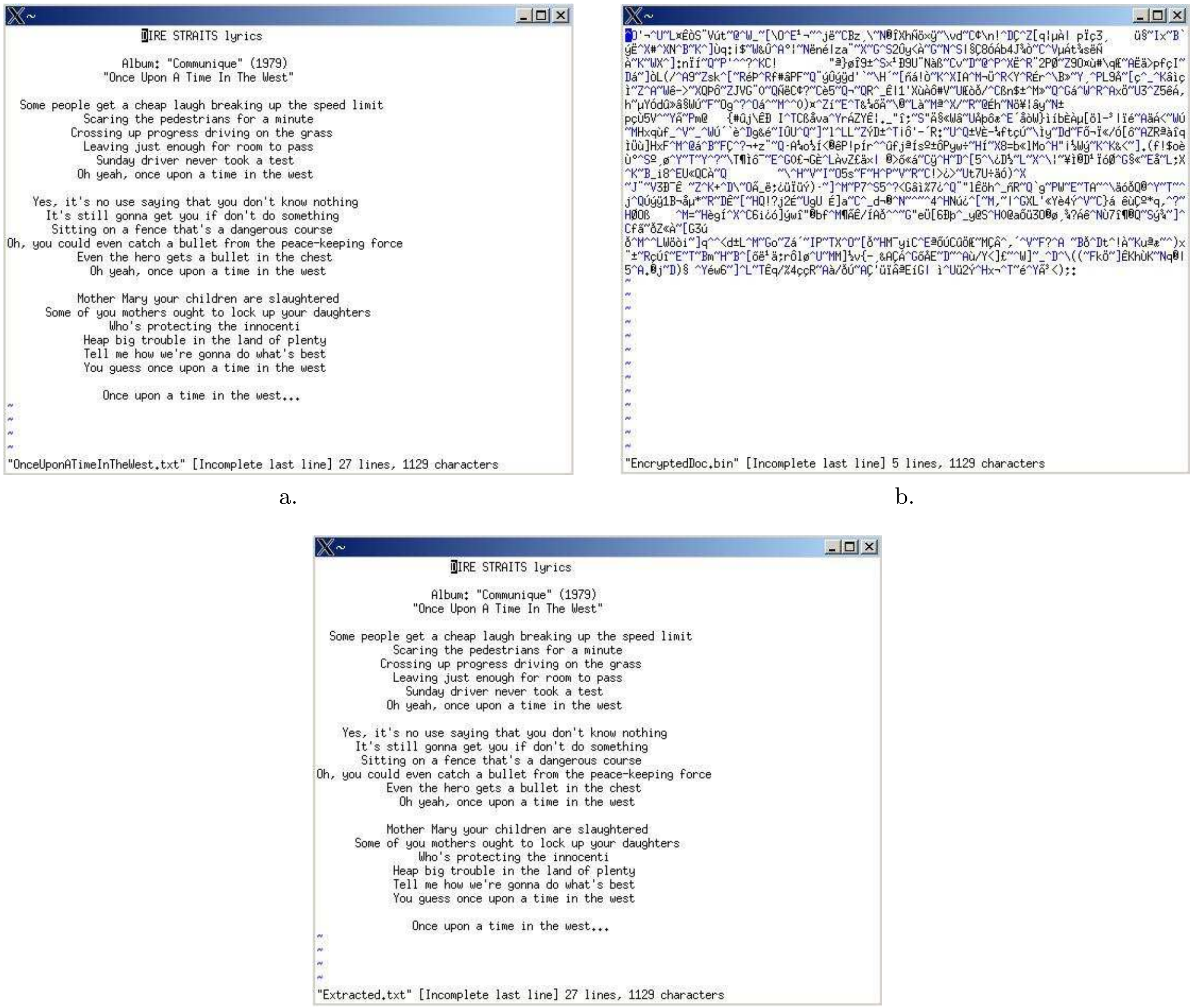
Step 5. Eve extracts the plaintext without the knowledge of the secret key K simply applying $P = C_{CBC} \oplus C_{OFB}$.

A variant of the Attack 1 can be launched even if the IV_{CBC} is not used in the OFB mode.

Attack 2.

Step 1. The attacker Eve knows the encryption of the string $\mathbf{0}$ i.e. she knows $C_{CBC} = e_{IV_{CBC},*}(\mathbf{0})$. She does not know the secret key K.

Step 2. Alice and Bob possess the secret key K, and decide to perform a secure communication using the OFB mode.



```
                    DIRE STRAITS lyrics

                  Album: "Communique" (1979)
               "Once Upon A Time In The West"

   Some people get a cheap laugh breaking up the speed limit
              Scaring the pedestrians for a minute
           Crossing up progress driving on the grass
              Leaving just enough for room to pass
                Sunday driver never took a test
               Oh yeah, once upon a time in the west

     Yes, it's no use saying that you don't know nothing
        It's still gonna get you if don't do something
          Sitting on a fence that's a dangerous course
Oh, you could even catch a bullet from the peace-keeping force
               Even the hero gets a bullet in the chest
                Oh yeah, once upon a time in the west

              Mother Mary your children are slaughtered
         Some of you mothers ought to lock up your daughters
                   Who's protecting the innocenti
              Heap big trouble in the land of plenty
              Tell me how we're gonna do what's best
               You guess once upon a time in the west

                    Once upon a time in the west...
~
~
~
~
"OnceUponATimeInTheWest.txt" [Incomplete last line] 27 lines, 1129 characters
```

a.

```
^O'¬^U^L¤ÊòS"Vút^@^W_^[\O^E¹¬^^jë^CBz¸\^N®îXhÑö×ÿ^\vd^C¢\n!^DÇ^Z[q¦µÀ¦ pÏç3¸    ü§^Ix^B`
ýË^X#^XN^B^K^]ùq:¡$^W&Û^A°¦^Nënélza"^X^G^S2Ûy<À^G^N^S¦§Ç8óÁb4J¾ò^C^VµÁt¾sëÑ
À^K^WX^]:nÏí^Q^P'^^?^KC!        "ª}øÎ9±^S×¹Ð9U"Naß^Cv^D^@^P^XË^R"2PØ^Z9O¤ù#\qŒ^AËä>pfçI^
Dá^]òL(/^A9^Zsk^[^RéP^Rf#âPF^Q"ýÛýÿd' `^\H´^[ñá!ò^K^XIA^M¬Ü^R<Y^Rér^\B»^Y¸^PL9Å^[ç^_^Kâìç
ì^Z^A^Wê->^XQPô^ZJVG"O^QÑëC¢?^Cè5^Q¬^QR^_Ê¦1'XùÀÔ#V^UŒòð/^CBn$±^M»^Q^Gá^W^R^Axö^U3^Z5êÁ,
h^µYódû»â§Wú^F^Og^?^Oá^^M^^O)¤^Zí^E^T&¼õÄ^\®^Là^Mª^X/^R^@Éh^Nö¥¦ây^N±
pçÙ5V^^YÃ^Pm@    {#ûj\ÊÐ I^TCßåva^YrÁZYÊ!¸_"î;^S"Ä§«Wâ^UÅþô æ^E´åòW}iíbÈÀµ[öl-³¦Ïé^AäÁ<^WÚ
^MHxqùf_^V^_^Wú´`è^Dg&é^IÔU^Q^]^l^LL^ZÝD±^TÌô'-´R:^U^Q±VÈ-¼ftçú^\ìy^Dd^Fõ¬Ï«/ó[ô^AZRªàîq
ÌÜù]HxF^M^@á^B^FÇ^?¬+z"^Q·A¼o½í<®êP!pír^^ûfjªís º±ÔPyw÷^Hí^X8=b«lMo^H"i½Wý^K^K&<^].(f!$oè
ù°^Sº¸ø^Y^T^Y^?^\T¶ìõ¯^E^GO£¬GÈ^LÀvZ£ä×¦ ®>õ«á^Cÿ^H^D^[5^\¿D½^L^X^\!^¥ì®D¹Ïó0^G§«^Eâ^L;X
^K^B_i8^EU«QCÀ^Q        ^\^H^V^I^O5s^F^H^P^V^R^C!>¿>^Ut7U÷äó)^X
^J"^V3Ð¯Ê ^Z^K+^D\^OÃ_ë;¿üÏüÝ)·^]^M^P7^S5^?<Gâì%7¿^Q""1Êöh^_ñR^Q`g^PW^E^TA^^\äóðQ®^Y^T^^
j^QÚýÿ1B¬åµ*^R^DÊ^[^HQ!?j2É^UgU É]a^C^_d¬®^N^^^^4^HNú¿^[^M,^¦^GXL'«Yè4Ý^V^C}á êùÇº*q,^?^
HØOß    ^M=^Hègí^X^C6i¿ó]ýwî"®bf^M¶ÃÊ/ÍAð^^^G"eÜ[6Ðþ^_y@S^HO@aõü3O®ø¸¾?Áê^NÙ7î¶®Q^Sý¾^]^
Cfã^ðZ«À^[G3ú
ð^M^^LWöòi^]q^^<d±L^M^Go^Zá´^IP^TX^O^[ð^HM¯yiC^EªõúCûöŒ^MÇÂ^¸´^V^F?^A ^Bð^Dt^!À^Kuªæ^^)x
"±^RçúÎ^E^T^Bm^H^B^[õë¹ä;rôlø^U^MM]½v{-¸&AÇÁ^GõÅE^D^^Aù/Y<]£^^W]^_^D^\((^Fkö^]ÊKhùK^Nq®¦
5^A.®j^D)§ ^Yéw6^]^L^TÊq/%4ççR^Aà/ðú^AÇ'üÏÂªEíG¦ ì^Uü2Ý^Hx¬^T^é^YÃ³<);:
~
~
~
~
~
~
~
~
~
~
~
~
"EncryptedDoc.bin" [Incomplete last line] 5 lines, 1129 characters
```

b.

```
                    DIRE STRAITS lyrics

                  Album: "Communique" (1979)
               "Once Upon A Time In The West"

   Some people get a cheap laugh breaking up the speed limit
              Scaring the pedestrians for a minute
           Crossing up progress driving on the grass
              Leaving just enough for room to pass
                Sunday driver never took a test
               Oh yeah, once upon a time in the west

     Yes, it's no use saying that you don't know nothing
        It's still gonna get you if don't do something
          Sitting on a fence that's a dangerous course
Oh, you could even catch a bullet from the peace-keeping force
               Even the hero gets a bullet in the chest
                Oh yeah, once upon a time in the west

              Mother Mary your children are slaughtered
         Some of you mothers ought to lock up your daughters
                   Who's protecting the innocenti
              Heap big trouble in the land of plenty
              Tell me how we're gonna do what's best
               You guess once upon a time in the west

                    Once upon a time in the west...
~
~
~
~
"Extracted.txt" [Incomplete last line] 27 lines, 1129 characters
```

c.

Fig. 2. Screen dumps for original, encrypted and extracted file.

Step 3. They chose to use IV that has never been used in previous OFB sessions but it happens that, that IV is also a block of the ciphertext C_{CBC} that Eve possess. According to the NIST recommendations, the use of such IV is allowed since it has never been used in OFB mode.

Step 4. Alice encrypts the plaintext P performing $C_{OFB} = OFB_{K,IV,encrypt}(P)$.

Step 5. Represented as concatenation of blocks, the ciphertext that Eve possess looks like: $C_{CBC} = C_1, \ldots, C_{j-1}, IV, C_{j+1}, \ldots$. She checks and finds out that the used IV is a block of her ciphertext, thus she cuts the first part of the ciphertext C_{CBC} (the fist part including IV) obtaining the string $C'_{CBC} = C_{j+1}, \ldots, C_N$. She extracts the plaintext (whole or a part of it) without the knowledge of the secret key K simply applying $P = C'_{CBC} \oplus C_{OFB}$.

If the lengths of C'_{CBC} and C_{OFB} are different, by convention, the output of $\oplus$ operation will have a length that is equal to the smaller length of both C'_{CBC} and C_{OFB}.

The third attack does not even require that the known plaintext have to consist of all zeroes. Actually it is enough the plaintext to have many zero-blocks parts i.e. to be of the form: $P = P_1, \ldots, P_{i_1-1}, \mathbf{0}_{i_1}, \ldots, \mathbf{0}_{i_2}, P_{i_2+1}, \ldots P_{i_3-1}, \mathbf{0}_{i_3}, \ldots, \mathbf{0}_{i_4}, P_{i_4+1}, \ldots$.

Attack 3.

Step 1. The attacker Eve knows the encryption of the string P i.e. she knows $C_{CBC} = e_{IV_{CBC},*}(P) = C_1, \ldots C_{i_1-1}, \mathbf{C}_{i_1}, \ldots, \mathbf{C}_{i_2}, C_{i_2+1}, \ldots C_{i_3-1}, \mathbf{C}_{i_3}, \ldots, \mathbf{C}_{i_4}, P_{i_4+1}, \ldots$. The parts of the ciphertext that are the result of the CBC encryption of the zero-block parts are denoted in bold. Eve does not know the secret key K.

Step 2. Alice and Bob possess the secret key K, and decide to perform a secure communication using the OFB mode.

Step 3. They chose to use IV that has never been used in previous OFB sessions but it happens that, that IV is a part of the bolded ciphertext blocks $\mathbf{C}_j$ that Eve possess. According to the NIST recommendations, the use of such IV is allowed since it has never been used in OFB mode.

Step 4. Alice encrypts the plaintext P performing $C_{OFB} = OFB_{K,IV,encrypt}(P)$.

Step 5. Simmilar as in the Attack 2, Eve extracts a part of the ciphertext C_{CBC} that corresponds to the used IV and the bolded ciphertext blocks $\mathbf{C}_j$, obtaining the string C'_{CBC}. She extracts the plaintext (whole or a part of it) without the knowledge of the secret key K simply applying $P = C'_{CBC} \oplus C_{OFB}$.

Example 1. In what follows we will demonstrate the Attack 1., with a concrete set of openssl commands and the corresponding screen dumps showing the effects of those commands.

We will use aes-128-cbc and aes-128-ofb options of the “enc” command in the openssl.

For the purpose of this example we have prepared a short plaintext file containing the song of Dire Straits, “Once Upon A Time In The West” from the album “Communiqué” from 1979 [4].

- By applying the command “`vi OnceUponATimeInTheWest.txt`” we can see the context of the file and the screen dump of that operation is shown in Figure 2a.
- The command “`dd if=/dev/zero of=zero.txt bs=4096 count=1024`” prepares a file of length 4 MBytes all with zeroes.
- The command “`openssl enc -aes-128-cbc -in zero.txt -out zero.bin -K 01234567890123456789012345678901 -iv 0123456789abcdef0123456789abcdef -nopad`” is the part of the known plaintext attack, where the file `zero.txt` is encrypted with CBC mode.

– The command "`openssl enc -aes-128-ofb -in OnceUponATimeInTheWest.txt -out EncryptedDoc.bin -K 01234567890123456789012345678901 -iv 0123456789abcdef0123456789abcdef -nopad`" encrypts the file `OnceUponATimeInTheWest.txt` in OFB mode with the same key and IV that were used in the CBC encryption. The resulting ciphertext file is named `EncryptedDoc.bin`.
– By applying the command "`vi EncryptedDoc.bin`" we can see the context of the encrypted file and the screen dump of that operation is shown in Figure 2b.
– The command "`./XORFiles zero.bin EncryptedDoc.bin Extracted.txt`" invokes a program that XORs two files and produces the third file. The length of the produced file is same as the length of the smaller file.
– By applying the command "`vi Extracted.txt`" we can see the content of the file and see the extracted plaintext. The screen dump of that operation is shown in Figure 2c.

4 Conclusions

In this paper we have represented two popular modes of operation of block ciphers (CBC and OFB) as quasigroup string transformations. Moreover we showed that OFB mode is a special case of CBC mode of operation where the encryption of a string of all zeroes is performed. From there, several attacks on the security of interchanged use of those two modes of operation were designed. From the formal point of view, in those attacks, NIST recommendations for the nature of IVs were followed, but still the attacks were able to reconstruct the plaintext without the knowledge of the secret key.

One possible update in the NIST recommendations for the modes of operation of block cipher would be to recommend IV for the OFB mode also to be unpredictable (rather than nonce). Another recommendation can be simply to forbid usage of the OFB mode.

One of the intentions of this paper is to provoke an interest for security analysis of modes of operation of block ciphers when those modes are interchangeably used. This paper shows that those modes are not at all independent and uncorrelated, and a plaintext extraction can be performed by knowing the ciphertext information from other modes of operation. Moreover, many modern software packages and libraries offer all five modes of operation and mistakes with improper interchanged use of those modes can happen.

A version of this paper has been sent to NIST, in order to initiate an update in the recommendations that are given in their publication [12].

References

1. Belousov, V.D.: Osnovi teorii kvazigrup i lup. (1967) "Nauka", Moskva
2. Crypto++ Library, http://www.cryptopp.com/
3. J. Dénes and A. D. Keedwell: Latin Squares. New Developments in the Theory and Applications, North-Holland Publishing Co., Amsterdam, 1991.
4. Dire Straits, "Once Upon A Time In The West" - Lirics, Album "Communique", 1979.
5. V. D. Gligor and P. Donescu, "Fast Encryption and Authentication: XCBC Encryption and XECB Authentication Modes", http://csrc.nist.gov/CryptoToolkit/modes/workshop1/papers/gligor-xcbc-xecb-2.pdf

6. J. Håstad and M. Näslund, “Key Feedback Mode: a Keystream Generator with Provable Security”, http://csrc.nist.gov/CryptoToolkit/modes/workshop1/papers/hastad-Naslund-kfb.pdf
7. C. S. Jutla, “Parallelizable Encryption Mode with Almost Free Message Integrity”, http://csrc.nist.gov/CryptoToolkit/modes/workshop2/presentations/iapm%20presentation/index.htm
8. L. R. Knudsen, “Block chaining modes of operation”, Reports in Informatics, ISSN 0333-3590, Department of Informatics, University of Bergen, Norway.
9. S. Markovski, D. Gligoroski, V. Bakeva, “Quasigroup String Processing: Part 1”, Maced. Acad. of Sci. and Arts, Sc. Math. Tech. Scien. **XX 1-2**, (1999) 13–28.
10. National Bureau of Standards, “DES modes of operation”, Federal Information Processing Standard (FIPS), Publication 81, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., December 1980.
11. National Institute of Standards and Technology, Modes of Operation Home page, http://csrc.nist.gov/CryptoToolkit/modes/
12. National Institute of Standards and Technology, Special Publication 800-38A 2001, “Recommendation for Block Cipher Modes of Operation Methods and Techniques”, 66 pages (December 2001).
13. The OpenSSL Project, http://www.openssl.org/
14. P. Rogaway, “OCB Mode: Parallelizable Authenticated Encryption”, Comments to NIST concerning AES Modes of Operation, Draft October 6 2000, http://csrc.nist.gov/CryptoToolkit/modes/workshop1/papers/rogaway-ocb1.pdf
15. J. D. H. Smith: An introduction to quasigroups and their representations, Chapman & Hall/CRC, ISBN 1-58488-537-8, 2007.