```
algorithm FFX.Encrypt($K, T, X$)
if $K \notin$ Keys or $T \notin$ Tweaks or
   $X \notin$ Chars$^*$ or $|X| \notin$ Lengths
   then return $\perp$
$n \leftarrow |X|$;  $\ell \leftarrow$ split($n$);  $r \leftarrow$ rnds($n$)
$A \leftarrow X[1 \,..\, \ell]$;  $B \leftarrow X[\ell+1 \,..\, n]$
for $i \leftarrow 0$ to $r-1$ do
    $C \leftarrow A \boxplus \mathsf{F}_K(n, T, i, B)$
    $A \leftarrow B$;  $B \leftarrow C$
return $A \,\|\, B$
```

```
algorithm FFX.Decrypt($K, T, Y$)
if $K \notin$ Keys or $T \notin$ Tweaks or
   $Y \notin$ Chars$^*$ or $|Y| \notin$ Lengths
   then return $\perp$
$n \leftarrow |Y|$;  $\ell \leftarrow$ split($n$);  $r \leftarrow$ rnds($n$)
$A \leftarrow Y[1 \,..\, \ell]$;  $B \leftarrow Y[\ell+1 \,..\, n]$
for $i \leftarrow r-1$ downto $0$ do
    $C \leftarrow B$;  $B \leftarrow A$
    $A \leftarrow C \boxminus \mathsf{F}_K(n, T, i, B)$
return $A \,\|\, B$
```

radix	a number radix $\in [2 \,..\, 2^{16}]$	alphabet is Chars $= \{0, 1, \ldots, \text{radix}-1\}$
Lengths	[minlen .. maxlen] where minlen $= 2$ if radix ≥ 10 and minlen $= 8$ otherwise; and maxlen $= 2^{32}-1$.	permitted message lengths
Keys	$\{0,1\}^{128}$	128-bit AES keys
Tweaks	$\text{BYTE}^{\leq \text{maxlen}}$ where maxlen $= 2^{32}-1$	tweaks are arbitrary byte strings
addition	1	blockwise addition
method	2	alternating Feistel
split (n)	$\lfloor n/2 \rfloor$	maximally balanced Feistel
rnds (n)	10	number of rounds
F	given below	AES-based round function

```
algorithm $\mathsf{F}_K(n, T, i, B)$
vers $\leftarrow 1$;  $t \leftarrow |T|_8$;  $\beta \leftarrow \lceil n/2 \rceil$;  $b \leftarrow \lceil \lceil \beta \log_2(\text{radix}) \rceil / 8 \rceil$;  $d \leftarrow 4\lceil b/4 \rceil$
if EVEN($i$) then $m \leftarrow \lfloor n/2 \rfloor$ else $m \leftarrow \lceil n/2 \rceil$

$P \leftarrow [\text{vers}]^1 \,\|\, [\text{method}]^1 \,\|\, [\text{addition}]^1 \,\|\, [\text{radix}]^3 \,\|\, [\text{rnds}(n)]^1 \,\|\, [\text{split}(n)]^1 \,\|\, [n]^4 \,\|\, [t]^4$
$Q \leftarrow T \,\|\, [0]^{(-t-b-1) \bmod 16} \,\|\, [i]^1 \,\|\, [\text{NUM}_{\text{radix}}(B)]^b$
$Y \leftarrow \text{CBC-MAC}_K(P \,\|\, Q)$
$Y \leftarrow$ first $d+4$ bytes of $(Y \,\|\, \text{AES}_K(Y \oplus [1]^{16}) \,\|\, \text{AES}_K(Y \oplus [2]^{16}) \,\|\, \text{AES}_K(Y \oplus [3]^{16}) \cdots)$
$y \leftarrow \text{NUM}_2(Y)$

$z \leftarrow y \bmod \text{radix}^m$
return $\text{STR}^m_{\text{radix}}(z)$
```