公募カテゴリーの事務局選出暗号1

暗号利用モード／メッセージ認証コードに関する事務局選出技術

CRYPTREC事務局

CRYPTREC
Cryptography Research and Evaluation Committees

事務局選出技術の選出基準

・国際標準技術など相互運用性上最低限必要な技術

・リストガイド作成時にWGによって安全性評価が確認されたもの

・リストガイド作成時にWGによって標準化動向が確認されたもの

CRYPTREC
Cryptography Research and Evaluation Committees

事務局選出技術カテゴリ

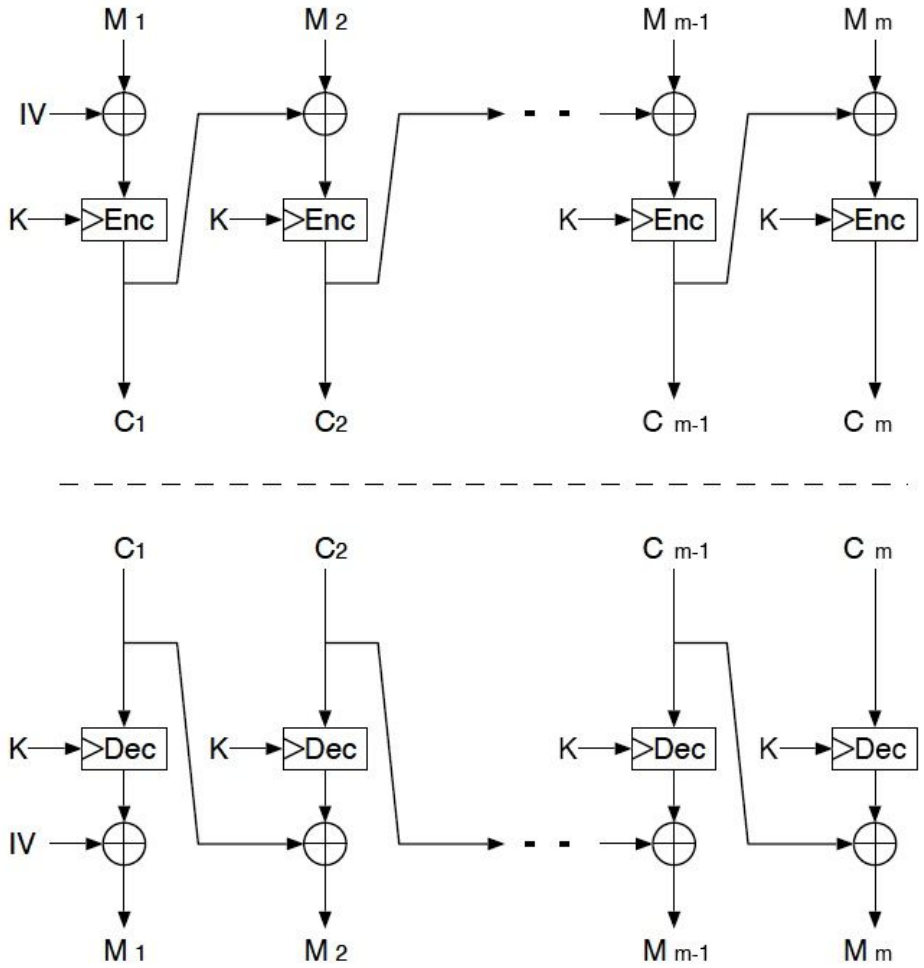
・ストリーム暗号　なし

・暗号利用モード 4件(ISO/IEC 10116, SP800-38A)

・メッセージ認証コード 3件(ISO/IEC 9797-1,-2)

CRYPTREC
Cryptography Research and Evaluation Committees

暗号利用モード１ CBC



・一般に良く使われている

・暗号化は並列処理不能だが
復号は可能

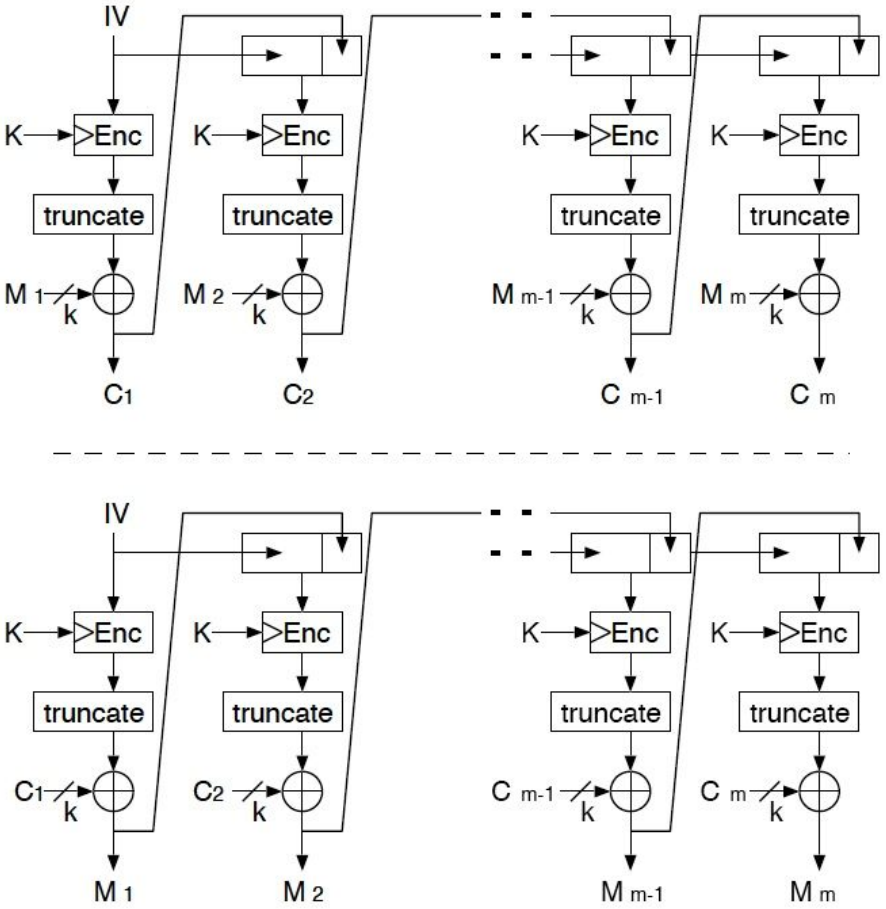
・”10パディング”推奨

・エラー伝播＝隣り合うブロック
へ影響

・初期値=予測不能制

CRYPTREC
Cryptography Research and Evaluation Committees

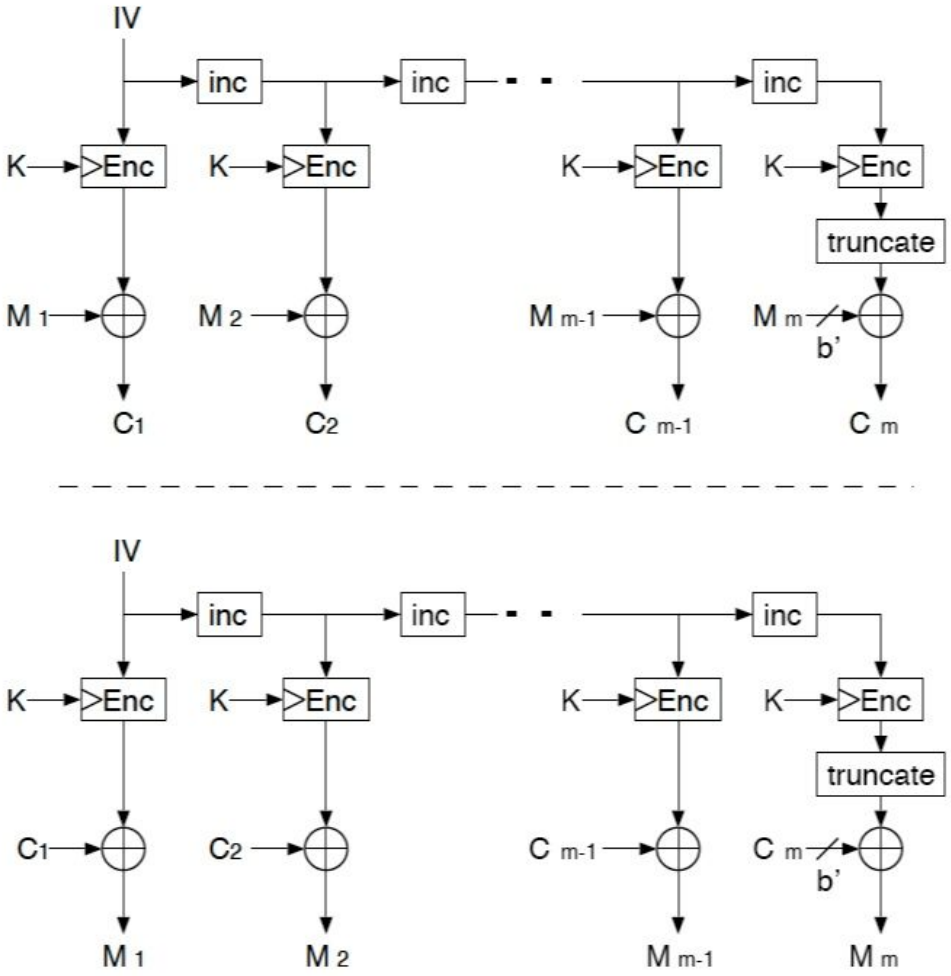
暗号利用モード 2 CFB



- 自己同期可能
- 並列処理不能
- 実行速度が遅い(復号回路は不要)
- メッセージ長が短いときパディング不要だが一般に必要
- 出力エラーは伝播が大きい
- 初期値=ナンス性(同じ鍵のもとで同じ初期値を使わない)

CRYPTREC
Cryptography Research and Evaluation Committees

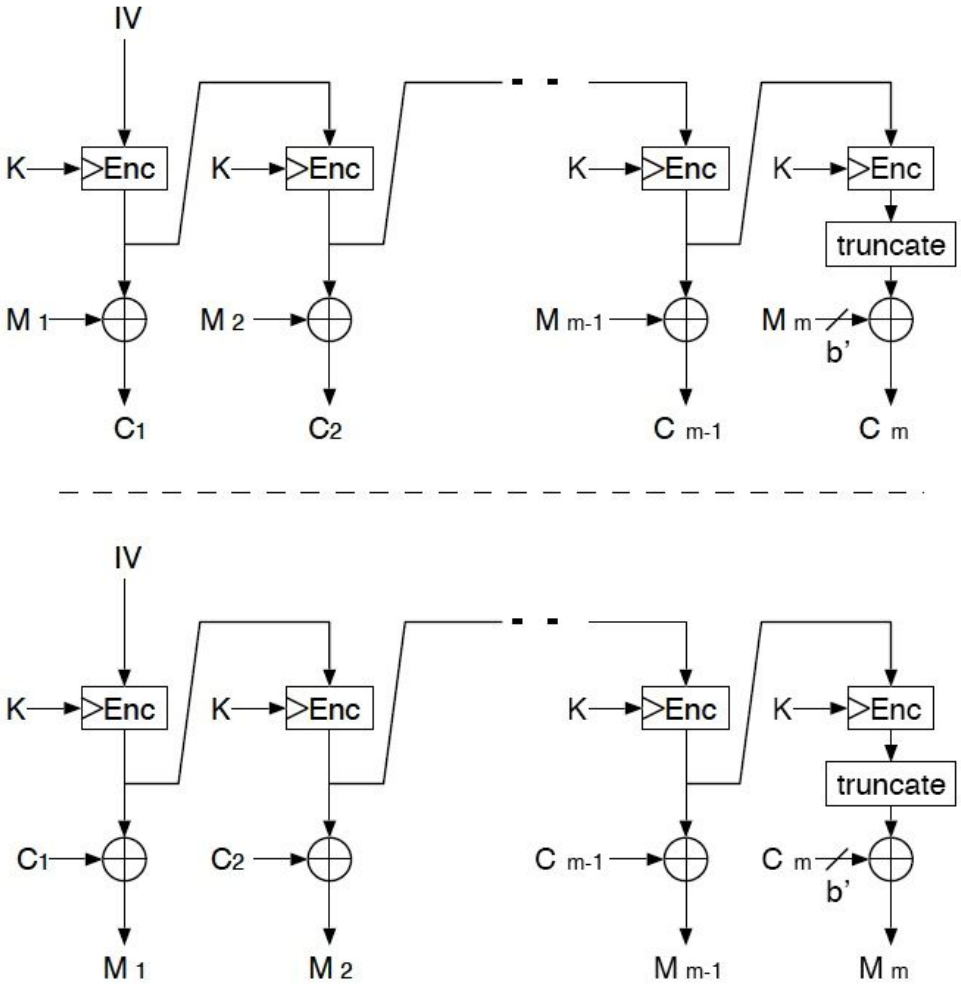
暗号利用モード3 CTR



- 並列処理可能
- 実行速度が早い(復号回路は不要)
- パディング不要
- エラー伝播は対応ビットのみ
- 初期値=ナンス性(同じカウンタ値を同一鍵内で使用しない)

CRYPTREC
Cryptography Research and Evaluation Committees

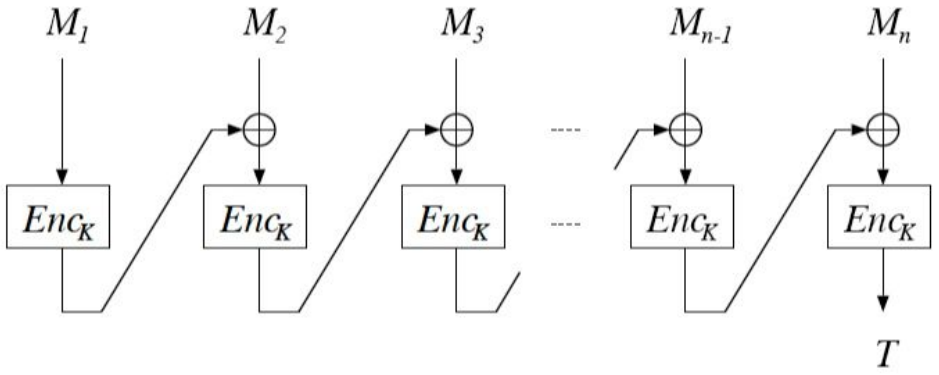
暗号利用モード4 OFB



- 並列処理不能
- 復号回路は不要
- パディング不要
- 出力エラーは伝播が大きい
- 初期値=ナンス性(同じ鍵のもとで同じ初期値を使わない)

CRYPTREC
Cryptography Research and Evaluation Committees

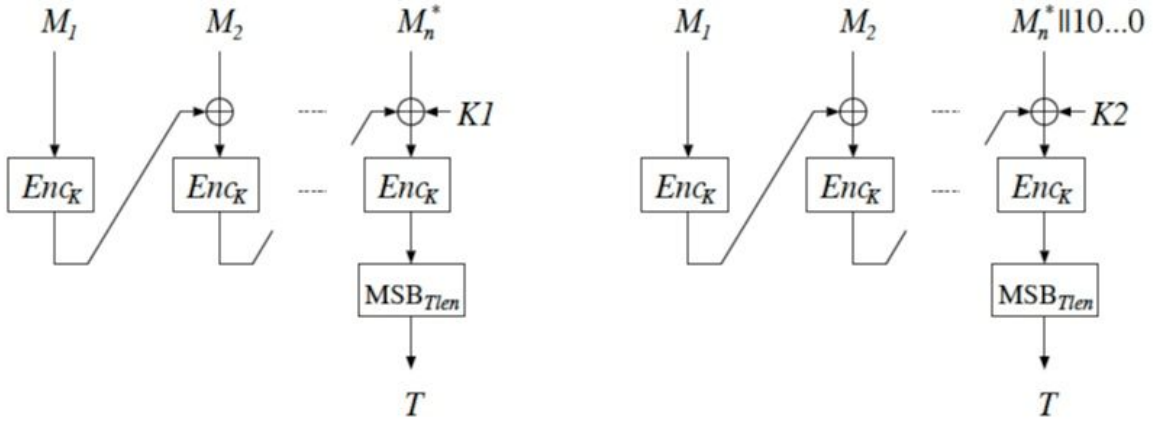
メッセージ認証コード 1 CBC-MAC



- DES用であるが汎用に使われている傾向にある。
- 偽造攻撃が良く知られている。安全に利用するためにメッセージ長の扱いに注意が必要。
- FIPS113は廃止された。
- リストガイドではISO 16609 TDESを利用したものが金融で利用されているため記述している。

CRYPTREC
Cryptography Research and Evaluation Committees

メッセージ認証コード 2　CMAC



・CBC-MACの欠点の解決

・128ビットブロック暗号の利用を想定しているため、64ビットブロック暗号の場合は利用するメッセージ長などに注意が必要

CRYPTREC
Cryptography Research and Evaluation Committees

メッセージ認証コード 3　HMAC

$$\mathrm{HMAC}(K, M, Tlen) = H((K_0 \oplus opad)||H((K_0 \oplus ipad)||M))$$

・公募はブロック暗号を利用したMACであるがHMACは利用普及が活発なため評価対象とした。

・HMACで利用するハッシュ関数はリストにて推奨しているものの利用を推定。

・プロトコルで特定のハッシュ関数の利用を指定している場合もある
(例: SSH(RFC 4253)ではHMAC-SHA1)。擬似ランダム関数と言えないハッシュ関数の利用は安全ではない場合もある。

CRYPTREC
Cryptography Research and Evaluation Committees