Towards Automatic Proofs for Symmetric Encryption Modes

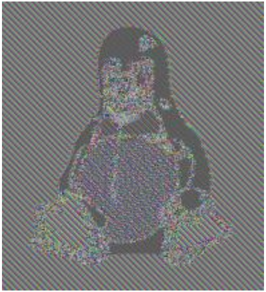
Martin Gagné[2] **Pascal Lafourcade**[1] Yassine Lakhnech[1]
Reihaneh Safavi-Naini[2]

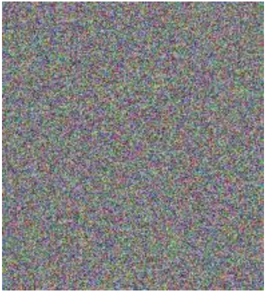
[1] Université Grenoble 1, CNRS, VERIMAG, FRANCE

[2] Department of Computer Science, University of Calgary, Canada

FCC: July 12th 2009, Port Jefferson USA.
(Work in progress)

Symmetric Encryption of Large Files





Indistinguishability (IND)

The adversary is not able to **guess in polynomial-time even a bit of the plain-text knowing the cipher-text**, notion introduced by S. Goldwasser and S.Micali ([GM84]).

IND for Symmetric Encryption Mode $\mathcal{E}_M$

- Sample $b \xleftarrow{R} \{0,1\}$.
- $(s, m_0, m_1) \xleftarrow{R} \mathcal{A}^{\mathcal{E}_M}(\eta)$
- $b' \xleftarrow{R} \mathcal{A}^{\mathcal{E}_M}(\eta, s, \mathcal{E}_M(m_b))$
- return b'.

Definition

$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{Ind}_{CPA}}(\eta) =$

$$Pr[b' \xleftarrow{R} \mathrm{Ind}_{CPA}^{b=1}(\mathcal{A}) : b' = 1] - Pr[b' \xleftarrow{R} \mathrm{Ind}_{CPA}^{b=0}(\mathcal{A}) : b' = 1]$$

$\mathcal{E}_M$ is IND-CPA secure if $\mathrm{Adv}_{\mathcal{A}}^{ind-CPA}(\eta)$ is negligible for any polynomial-time adversary $\mathcal{A}^{\mathcal{E}_M}$.

Related Works

- Bellare et al, in 1997, propose a Concrete Security Treatment of Symmetric Encryption
- Bellare'04, Shoup'04, Halevi ... have game-based approach
- G. Barthe et al provide formal models of the Generic Model and the ROM in the Coq proof assistant, and prove hardness of the discrete logarithm, security of several schemes.
- R. Corin and J. Den Hartog'06 propose a Hoare-style proof system for game-based cryptographic proofs.
- B. Blanchet develops CryptoVerif security proofs within the game-based, based on observational equivalence.
- A. Datta et al. present a computationally sound compositional logic for key exchange protocols.
- CDELL 08 : Towards Automated Proofs for Asymmetric Encryption Schemes.

Outline

Outline

Block Cipher Modes

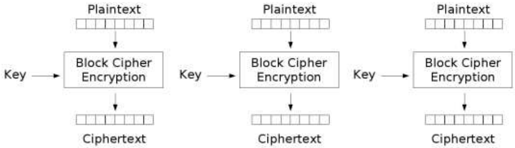
NIST standard

- Electronic Code Book (ECB)
- Cipher Block Chaining (CBC)
- Cipher FeedBack mode (CFB)
- Output FeedBack (OFB), and
- Counter mode (CTR).

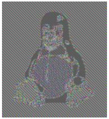
Others

DMC,CBC-MAC, IACBC, IAPM, XCB ,TMAC, HCTR, HCH, EME, EME*, PEP, OMAC, TET, CMC, GCM, EAX, XEX, TAE, TCH, TBC, CCM, ABL4

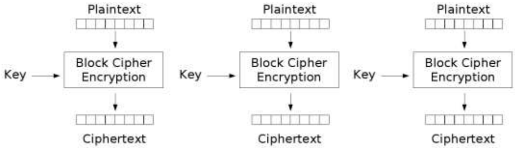
Each block of the same length is encrypted separately.



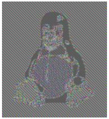
Electronic Codebook (ECB) mode encryption

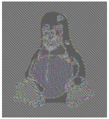


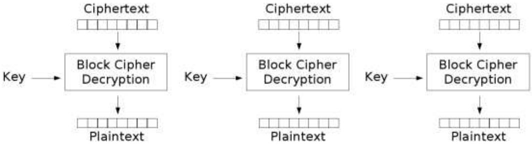
Each block of the same length is encrypted separately.



Electronic Codebook (ECB) mode encryption







Electronic Codebook (ECB) mode decryption

Attack on ECB

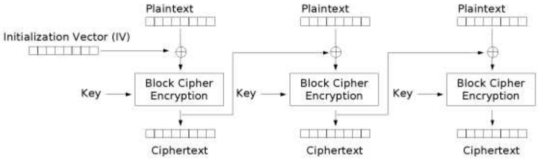
Adversary $A^{\mathcal{E}_K(LR(.,.,b))}$
$M_0 \leftarrow 0^n || 1^n$;
$M_1 \leftarrow 0^{2n}$;
$C[1]C[2] \leftarrow \mathcal{E}_K(LR(M_0, M_1, b))$
If $C[1] = C[2]$ then return 1 else return 0

$$\mathcal{E}_K(LR(m_l, m_r, b)) = \begin{cases} \mathcal{E}_K(m_l) & if\ \ b = 1 \\ \mathcal{E}_K(m_r) & if\ \ b = 0 \end{cases}$$

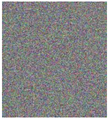
$C[i]$ denotes the i-th block of a string C.

$$Adv_{\mathcal{SE}}^{IND-CPA}(A) = 1 - 0 = 1$$

Cipher Block Chaining (CBC) Encryption

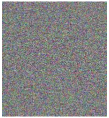


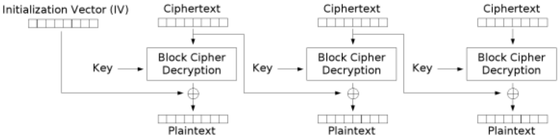
Cipher Block Chaining (CBC) mode encryption



$$C_i = E_K(P_i \oplus C_{i-1}), C_0 = IV$$

Cipher Block Chaining (CBC) Decryption





Cipher Block Chaining (CBC) mode decryption

$$P_i = D_K(C_i) \oplus C_{i-1}, C_0 = IV$$

CBC and others

CBC	CTR	OFB	CFB
$IV \xleftarrow{\$} \mathcal{U};$	$IV \xleftarrow{\$} \mathcal{U};$	$IV \xleftarrow{\$} \mathcal{U};$	$IV \xleftarrow{\$} \mathcal{U};$
$z_1 := IV \oplus m_1;$	$z_1 := \mathcal{E}(IV+1);$	$z_1 := \mathcal{E}(IV);$	$z_1 := \mathcal{E}(IV);$
$c_1 := \mathcal{E}(z_1);$	$c_1 := m_1 \oplus z_1;$	$c_1 := m_1 \oplus z_1;$	$c_1 := m_1 \oplus z_1;$
$z_2 := c_1 \oplus m_2;$	$z_2 := \mathcal{E}(IV+2);$	$z_2 := \mathcal{E}(z_1);$	$z_2 := \mathcal{E}(c_1);$
$c_2 := \mathcal{E}(z_2);$	$c_2 := m_2 \oplus z_2;$	$c_2 := m_2 \oplus z_2;$	$c_2 := m_2 \oplus z_2;$
$z_3 := c_2 \oplus m_3;$	$z_3 := \mathcal{E}(IV+3);$	$z_3 := \mathcal{E}(z_2);$	$z_3 := \mathcal{E}(c_2);$
$c_3 := \mathcal{E}(z_3);$	$c_3 := m_3 \oplus z_3;$	$c_3 := m_3 \oplus z_3;$	$c_3 := m_3 \oplus z_3;$

Outline

Grammar

$$
\begin{aligned}
\mathsf{c} \quad ::= \quad & x \xleftarrow{\$} \mathcal{U} \mid x := \mathcal{E}(y) \mid x := \mathcal{E}^{-1}(y) \\
& \mid x := y \oplus z \mid x := y \| z \mid x := y[n, m] \\
& \mid x := y + 1 \mid c_1 ; c_2
\end{aligned}
$$

Generic Encryption Mode

Definition

A generic encryption mode M is represented by

$$\mathcal{E}_M(m_1|\ldots|m_p, c_0|\ldots|c_p) : \textbf{var } \vec{x}; \mathrm{c}$$

$$\begin{array}{l}
\mathcal{E}_{CBC}(m_1|m_2|m_3, IV|c_1|c_2|c_3) : \\
\textbf{var } z_1, z_2, z_3; \\
IV \xleftarrow{\$} \mathcal{U}; \\
z_1 := IV \oplus m_1; \\
c_1 := \mathcal{E}(z_1); \\
z_2 := c_1 \oplus m_2; \\
c_2 := \mathcal{E}(z_2); \\
z_3 := c_2 \oplus m_3; \\
c_3 := \mathcal{E}(z_3);
\end{array}$$

Outline

Predicates

$$\psi ::= \mathrm{Indis}(\nu x; V) \mid F(e) \mid \mathrm{E}(\mathcal{E}, e) \mid Rcounter(e)$$
$$\varphi ::= \mathrm{true} \mid \varphi \wedge \varphi \mid \psi,$$

Indis$(\nu x; V)$: any adversary has negligible probability to distinguish whether he is given results of computations performed using the value of x or a random value, when he is given the values of the variables in V.

$F(e)$: means e is a fresh random value.

$\mathrm{E}(\mathcal{E}, l)$: the probability that the values of the expression e_i in the list l have been submitted to the symmetric encryption $\mathcal{E}$ is negligible.

$RCounter(e)$: means that e is the most recent value of a counter that started at a fresh random value.

Remark:

$$F(e) \Rightarrow \mathrm{Indis}(\nu e)$$

$$F(e) \Rightarrow \mathrm{E}(\mathcal{E}, e)$$

More Formally

- $X \models \text{true}$.
- $X \models \varphi \wedge \varphi'$ iff $X \models \varphi$ and $X \models \varphi'$.
- $X \models \text{Indis}(\nu x; V)$ iff $[u \stackrel{r}{\leftarrow} \mathcal{U}; (S, \mathcal{E}) \stackrel{r}{\leftarrow} X : (S(u, V), \mathcal{E})] \sim [(S, \mathcal{E}) \stackrel{r}{\leftarrow} X : (S(x, V), \mathcal{E})]$
- $X \models \text{E}(\mathcal{E}, I)$ iff for all $e \in I$, $\Pr[(S, \mathcal{E}) \stackrel{r}{\leftarrow} X : S(e) \in S(\mathcal{T}_{\mathcal{E}}).dom]$ is negligible.
- $X \models F(e)$ iff $e \in S(F)$.
- $X \models RCounter(e)$ iff $e \in S(C)$.

Semantic of the Programming Language

$$[\![x \xleftarrow{r} \mathcal{U}]\!](S,\mathcal{E}) = [u \xleftarrow{r} \mathcal{U} : (S\{x \mapsto u, F \mapsto F \cup \{x\}\}, \mathcal{E})]$$

$$[\![x := \mathcal{E}(y)]\!](S,\mathcal{E}) = \begin{cases} \delta(S\{x \mapsto v, F \mapsto F \cup \{x\} \setminus \{y\}\}, \mathcal{E}) \text{ if } (S(y), v) \in \mathcal{T}_{\mathcal{E}} \\ \delta(S\{x \mapsto v, F \mapsto F \cup \{x\} \setminus \{y\}, \mathcal{T}_{\mathcal{E}} \mapsto S(\mathcal{T}_{\mathcal{E}}) \cdot (S(y), v)\}, \mathcal{E}) \text{ if } (S(y), v) \notin \mathcal{T}_{\mathcal{E}} \\ \qquad \text{and } v = \mathcal{E}(S(y)) \end{cases}$$

$$[\![x := \mathcal{E}^{-1}(y)]\!](S,\mathcal{E}) = \delta(S\{x \mapsto \mathcal{E}^{-1}(S(y)), F \mapsto F \setminus \{x, y\}\}, \mathcal{E})$$

$$[\![x := y \oplus z]\!](S,\mathcal{E}) = \delta(S\{x \mapsto S(y) \oplus S(z), F \mapsto F \setminus \{x, y, z\}\}, \mathcal{E})$$

$$[\![x := y||z]\!](S,\mathcal{E}) = \delta(S\{x \mapsto S(y)||S(z), F \mapsto F \setminus \{x, y, z\}\}, \mathcal{E})$$

$$[\![x := y[n,m]]\!](S,\mathcal{E}) = \delta(S\{x \mapsto S(y)[n,m], F \mapsto F \setminus \{x, y\}\}, \mathcal{E})$$

$$[\![x := y + 1]\!](S,\mathcal{E}) = \begin{cases} \delta(S\{x \mapsto S(y)+1, C \mapsto C \cup \{x\} \setminus \{y\}, F \mapsto F \setminus \{x, y\}\}, \mathcal{E}) \text{ if } y \in F \text{ or } y \in C \\ \delta(S\{x \mapsto S(y)+1, F \mapsto F \setminus \{x, y\}\}, \mathcal{E}) \text{ otherwise} \end{cases}$$

$$[\![c_1; c_2]\!] = [\![c_2]\!] \circ [\![c_1]\!]$$

Main Result

Prop

*Let $\mathcal{E}_M(m_1|\ldots|m_p, c_0|\ldots|c_p)$: **var** $\vec{x}; c$ be a generic encryption mode, and let $IO = \{m_1, \ldots, m_p, c_0, \ldots, c_p\}$. Then $\mathcal{E}_M$ is IND-CPA secure, if $\{true\}c \bigwedge_{i=0}^{i=p}\{Indis(\nu c_i; IO)\}$ is valid.*

Proof in progress.

Outline

Random Assignment:

- (R1) $\{true\}\ x \xleftarrow{\$} \mathcal{U}\ \{F(x)\}$
- (R2) $\{\mathrm{Indis}(\nu y; V)\}\ x \xleftarrow{\$} \mathcal{U}\ \{\mathrm{Indis}(\nu y; V, x)\}$

Using Lemma and (R1) we obtain $\{\mathrm{Indis}(\nu x)\}$ and $\{\mathrm{E}(\mathcal{E}, x)\}$, this combination is often used in the examples.

Block Cipher Rules:

- (B1) $\{\mathsf{E}(\mathcal{E}, y)\}\ x := \mathcal{E}(y)\ \{F(x)\}$
- (B2) $\{\mathsf{Indis}(\nu y; V)\}\ x := \mathcal{E}(y)\ \{\mathsf{Indis}(\nu y; V)\}$
- (B3) $\{Rcounter(y)\}\ x := \mathcal{E}(y)\ \{Rcounter(y)\}$

Increment:

- (I1) $\{F(y)\}\ x := y + 1$
  $\{RCounter(x)\} \wedge \{\mathrm{E}(\mathcal{E}, x)\} \wedge \{\mathrm{Indis}(\nu y; \mathrm{Var} - x)\}$
- (I2) $\{RCounter(y)\}\ x := y + 1\ \{RCounter(x)\} \wedge \{\mathrm{E}(\mathcal{E}, x)\}$
- (I3) $\{\mathrm{Indis}(\nu z; V)\}\ x := y + 1\ \{\mathrm{Indis}(\nu z; V - x)\}$ if $z \neq x, y$ and $y \notin V$

Xor operator:

- (X1) $\{\text{Indis}(\nu y; V, y, z)\} x := y \oplus z \{\text{Indis}(\nu x; V, x, z)\}$,
- (X2) $\{\text{Indis}(\nu y; V, x)\} x := y \oplus z \{\text{Indis}(\nu y; V)\}$,
- (X3) $\{\text{Indis}(\nu t; V, y, z)\}\ x := y \oplus z\ \{\text{Indis}(\nu t; V, x, y, z)\}$ if $t \neq x, y, z$
- (X4) $\{F(y)\}\ x := y \oplus z\ \{\text{E}(\mathcal{E}, x, y)\}$ if $y \neq z$

Concatenation:

- (C1) $\{\mathsf{Indis}(\nu y; V, y, z)\} \wedge \{\mathsf{Indis}(\nu z; V, y, z)\}\ x := y \| z$ $\{\mathsf{Indis}(\nu x; V, x)\}$ if $y, z \notin V$
- (C2) $\{\mathsf{Indis}(\nu t; V, y, z)\}\ x := y \| z\ \{\mathsf{Indis}(\nu t; V, x, y, z)\}$ if $t \neq x, y, z$

Generic preservation rules:

The following rules are sound, when $x \notin V$. Assume that $z \neq x, w, v$ and c is either $x \xleftarrow{\$} \mathcal{U}$, $x := w \| v$, $x := w \oplus v$, $x := \mathcal{E}(w)$ or $x := w + 1$:

- (G1) $\{\mathrm{Indis}(\nu z; V)\}$ c $\{\mathrm{Indis}(\nu z; V)\}$ provided c is not $x := w + 1$
- (G2) $\{\mathrm{E}(\mathcal{E}, z)\}$ c $\{\mathrm{E}(\mathcal{E}, z)\}$
- (G3) $\{RCounter(z)\}$ c $\{RCounter(z)\}$
- (G4) $\{F(z)\}$ c $\{F(z)\}$

Outline

Example: CBC

$\mathcal{E}_{CBC}(m_1|m_2|m_3, IV|c_1|c_2|c_3)$

var IV, z_1, z_2, z_3;

$IV \xleftarrow{\$} \mathcal{U}$;	$\{\mathrm{Indis}(\nu IV; \mathrm{Var})\} \wedge F(IV) \wedge \{\mathrm{E}(\mathcal{E}, IV)\}$	(R1)
$z_1 := IV \oplus m_1$;	$\{\mathrm{Indis}(\nu IV; \mathrm{Var} - z_1)\} \wedge \{\mathrm{E}(\mathcal{E}, z_1, IV)\}$	(X2)(X4)
$c_1 := \mathcal{E}(z_1)$;	$\{\mathrm{Indis}(\nu IV; \mathrm{Var} - z_1)\}$	(G1)
	$\wedge\{\mathrm{Indis}(\nu c_1; \mathrm{Var})\} \wedge \{F(c_1)\}$	(B1)
$z_2 := c_1 \oplus m_2$;	$\{\mathrm{Indis}(\nu IV; \mathrm{Var} - z_1)\}$	(G1)
	$\wedge\{\mathrm{Indis}(\nu c_1; \mathrm{Var} - z_2)\} \wedge \{\mathrm{E}(\mathcal{E}, z_1, c_1)\}$	(X2)(X4)
$c_2 := \mathcal{E}(z_2)$;	$\{\mathrm{Indis}(\nu IV; \mathrm{Var} - z_1)\} \wedge \{\mathrm{Indis}(\nu c_1; \mathrm{Var} - z_2)\}$	(G1)
	$\wedge\{Indis(\nu c_2; \mathrm{Var})\} \wedge F(c_2)$	(B1)
$z_3 := c_2 \oplus m_3$;	$\{\mathrm{Indis}(\nu IV; \mathrm{Var} - z_1)\} \wedge \{\mathrm{Indis}(\nu c_1; \mathrm{Var} - z_2)\}$	(G1)
	$\wedge\{\mathrm{Indis}(\nu c_2; \mathrm{Var} - z_3)\} \wedge \{\mathrm{E}(\mathcal{E}, z_3, c_3)\}$	(X2)(X4)
$c_3 := \mathcal{E}(z_3)$;	$\{\mathrm{Indis}(\nu IV; \mathrm{Var} - z_1)\} \wedge \{\mathrm{Indis}(\nu c_1; \mathrm{Var} - z_2)\}$	(G1)
	$\wedge\{\mathrm{Indis}(\nu c_2; \mathrm{Var} - z_3)\} \wedge \{Indis(\nu c_3; \mathrm{Var})\}$	(B1)

Outline

Summary

- Generic Encryption Mode
- New predicats
- Hoare Logic for proving generic encryption mode IND-CPA
- Automatic proof of CBC, FBC, OFB CFB.

Future Works

- Hybrid encryption
- using LSFR (Dual Encryption Mode)
- using Hash function
- using mathematics (GMC)
- IND-CCA ?
  Desai 2000: New Paradigms for Constructing Symmetric Encryption Schemes Secure against Chosen-Ciphertext Attack

Thank you for your attention.

Questions ?