CS 6260
Applied Cryptography

Alexandra (Sasha) Boldyreva

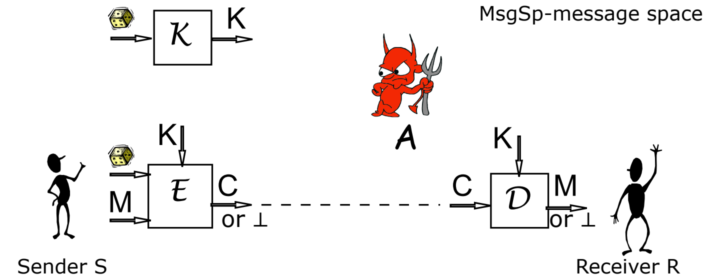
Symmetric encryption, encryption modes, security notions.

Symmetric encryption schemes

A scheme SE is specified by a key generation algorithm $\mathcal{K}$, an encryption algorithm $\mathcal{E}$, and a decryption algorithm $\mathcal{D}$.

SE=$(\mathcal{K},\mathcal{E},\mathcal{D})$

MsgSp-message space



It is required that for every M∈MsgSp and every K that can be output by $\mathcal{K}$, $\mathcal{D}$(K,$\mathcal{E}$(K,M))=M

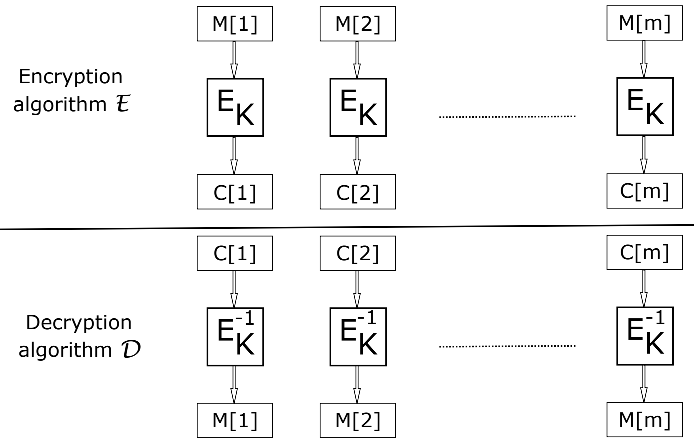
- Often the key generation algorithm simply picks a random string from some key space KeySp (e.g. $\{0,1\}^k$ for some integer k).
  - In this case we will say that a scheme SE is defined by KeySp and two algorithms: SE=(KeySp,$\mathcal{E}$,$\mathcal{D}$)
- The encryption algorithm can be either
  - randomized (take as input a random string)
  - or stateful (take as input some state (e.g. counter) that it can update)

Block cipher modes of operation

- Modes of operation define how to use a block cipher to encrypt long messages
- We will often assume that the message space consists of messages whose length is multiple of a block length

Electronic Code Book (ECB) mode

Let E:$\{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a block cipher. ECB=($\{0,1\}^k$,$\mathcal{E}$,$\mathcal{D}$):



Electronic Code Book (ECB) mode

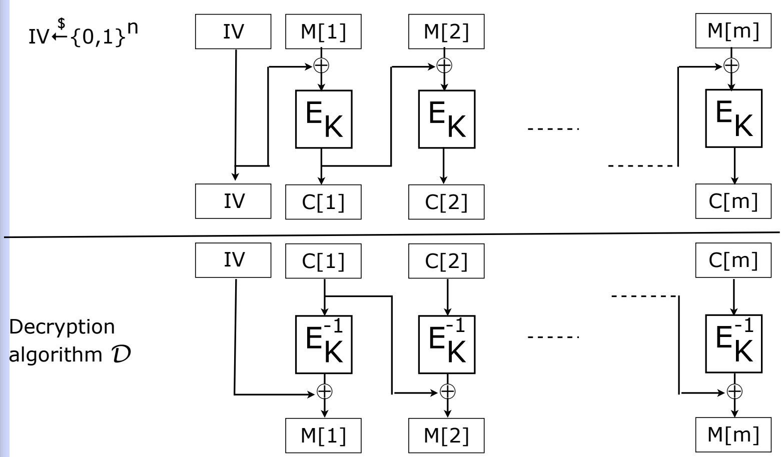
algorithm $\mathcal{E}_K(M)$
  if $(|M| \bmod n \neq 0$ or $|M| = 0)$ **then return** $\perp$
  Break M into n-bit blocks $M[1] \cdots M[m]$
  for $i \leftarrow 1$ to m **do**
    $C[i] \leftarrow E_K(M[i])$
  $C \leftarrow C[1] \cdots C[m]$
  return C

algorithm $\mathcal{D}_K(C)$
  if $(|C| \bmod n \neq 0$ or $|C| = 0)$ **then return** $\perp$
  Break C into n-bit blocks $C[1] \cdots C[m]$
  for $i \leftarrow 1$ to m **do**
    $M[i] \leftarrow E_K^{-1}(C[i])$
  $M \leftarrow M[1] \cdots M[m]$
  return M

Cipher-block chaining (CBC) mode with random IV

Let E:$\{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a block cipher. CBC\$=($\{0,1\}^k$,$\mathcal{E}$,$\mathcal{D}$):

Encryption algorithm $\mathcal{E}$



Cipher-block chaining (CBC) mode with random IV

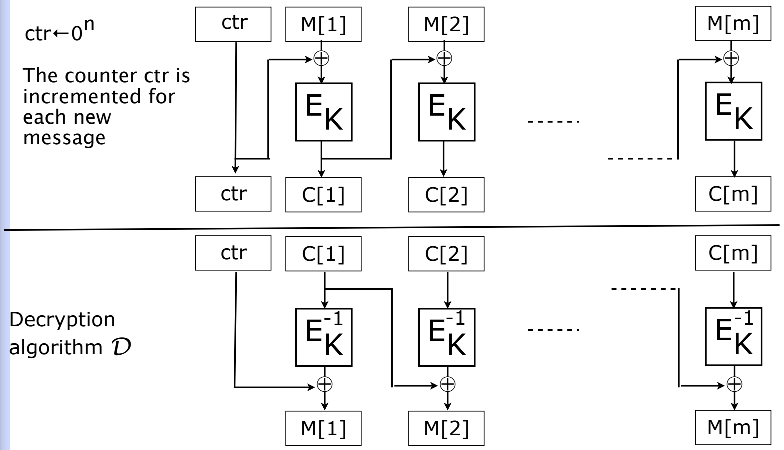
algorithm $\mathcal{E}_K(M)$
  if $(|M| \bmod n \neq 0$ or $|M| = 0)$ **then return** $\perp$
  Break M into n-bit blocks $M[1] \cdots M[m]$
  $C[0] \leftarrow \mathrm{IV} \stackrel{\$}{\leftarrow} \{0,1\}^n$
  for $i \leftarrow 1$ to m **do**
    $C[i] \leftarrow E_K(C[i-1] \oplus M[i])$
  $C \leftarrow C[1] \cdots C[m]$
  return $\langle \mathrm{IV}, C \rangle$

algorithm $\mathcal{D}_K(\langle \mathrm{IV}, C \rangle)$
  if $(|C| \bmod n \neq 0$ or $|M| = 0)$ **then return** $\perp$
  Break C into n-bit blocks $C[1] \cdots C[m]$
  $C[0] \leftarrow \mathrm{IV}$
  for $i \leftarrow 1$ to m **do**
    $M[i] \leftarrow E_K^{-1}(C[i]) \oplus C[i-1])$
  $M \leftarrow M[1] \cdots M[m]$
  return M

Stateful Cipher-block chaining (CBC) mode with counter IV

Let $E:\{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a block cipher. CBCC=$(\{0,1\}^k, \mathcal{E}, \mathcal{D})$:

Encryption algorithm $\mathcal{E}$



Stateful Cipher-block chaining (CBC) mode with counter IV

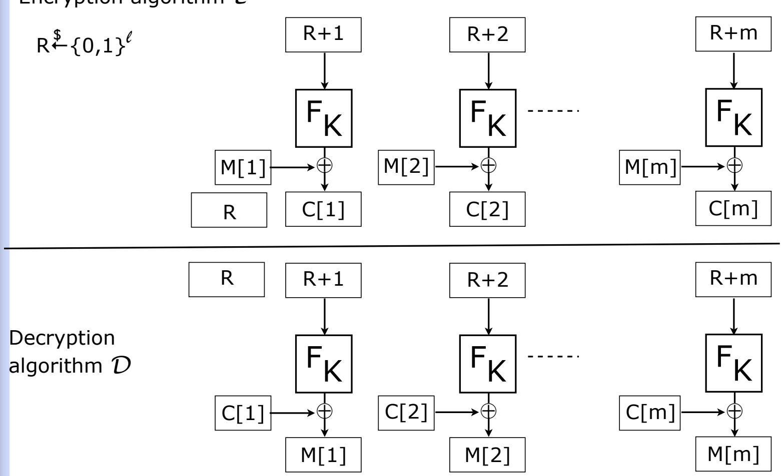
algorithm $\mathcal{E}_K(M)$
  static $ctr \leftarrow 0$
  if $(|M| \bmod n \neq 0$ or $|M| = 0)$ **then return** $\perp$
  Break M into n-bit blocks $M[1]\cdots M[m]$
  if $ctr \geq 2^n$ **then return** $\perp$
  $C[0] \leftarrow \mathrm{IV} \leftarrow [ctr]_n$
  for $i \leftarrow 1$ to m **do**
    $C[i] \leftarrow E_K(C[i-1] \oplus M[i])$
  $C \leftarrow C[1]\cdots C[m]$
  $ctr \leftarrow ctr + 1$
  return $\langle \mathrm{IV}, C\rangle$

algorithm $\mathcal{D}_K(\langle \mathrm{IV}, C\rangle)$
  if $(|C| \bmod n \neq 0$ or $|C| = 0)$ **then return** $\perp$
  Break C into n-bit blocks $C[1]\cdots C[m]$
  if $\mathrm{IV} + m > 2^n$ **then return** $\perp$
  $C[0] \leftarrow \mathrm{IV}$
  for $i \leftarrow 1$ to m **do**
    $M[i] \leftarrow E_K^{-1}(C[i]) \oplus C[i-1])$
  $M \leftarrow M[1]\cdots M[m]$
  return M

Randomized counter mode (CTR$)

Let $F:\{0,1\}^k \times \{0,1\}^\ell \rightarrow \{0,1\}^L$ be a function family. CBC$=$(\{0,1\}^k, \mathcal{E}, \mathcal{D})$:

Encryption algorithm $\mathcal{E}$



Randomized counter mode (CTR$)

algorithm $\mathcal{E}_K(M)$
  $m \leftarrow \lceil |M|/L \rceil$
  $R \xleftarrow{\$} \{0,1\}^\ell$
  $Pad \leftarrow F_K(R+1) \,\|\, F_K(R+2) \,\|\, \cdots \,\|\, F_K(R+m)$
  $Pad \leftarrow$ the first $|M|$ bits of Pad
  $C' \leftarrow M \oplus Pad$
  $C \leftarrow R \,\|\, C'$
  return C

algorithm $\mathcal{D}_K(C)$
  if $|C| < \ell$ **then return** $\perp$
  Parse C into $R \,\|\, C'$ where $|R| = \ell$
  $m \leftarrow \lceil |C'|/L \rceil$
  $Pad \leftarrow F_K(R+1) \,\|\, F_K(R+2) \,\|\, \cdots \,\|\, F_K(R+m)$
  $Pad \leftarrow$ the first $|C'|$ bits of Pad
  $M \leftarrow C' \oplus Pad$
  return M

Stateful counter mode (CTRC)

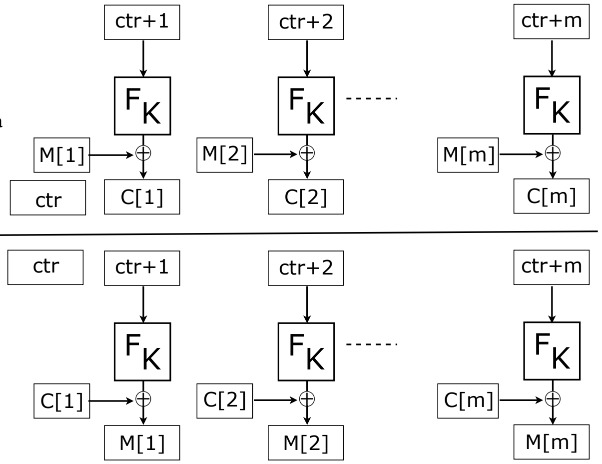
Let F:{0,1}^{k}×{0,1}$^\ell$→{0,1}^{L} be a function family. CBC$=({0,1}^{k},$\mathcal{E}$,$\mathcal{D}$):

Encryption algorithm $\mathcal{E}$

ctr is initially 0^ℓ

A current counter ctr is maintained as a state

Decryption algorithm $\mathcal{D}$



Stateful counter mode (CTRC)

algorithm $\mathcal{E}_K(M)$
static $ctr \leftarrow 0$
$m \leftarrow \lceil |M|/L \rceil$
If $ctr + m \geq 2^\ell$ **then return** $\perp$
$Pad \leftarrow F_K(ctr+1) \,\|\, F_K(ctr+2) \,\|\, \cdots \,\|\, F_K(ctr+m)$
$Pad \leftarrow$ the first $|M|$ bits of Pad
$C \leftarrow M \oplus Pad$
$ctr \leftarrow ctr + m$
return $\langle ctr - m, C \rangle$

algorithm $\mathcal{D}_K(\langle i, C \rangle)$
$m \leftarrow \lceil |C|/L \rceil$
$Pad \leftarrow F_K(i+1) \,\|\, F_K(i+2) \,\|\, \cdots \,\|\, F_K(i+m)$
$Pad \leftarrow$ the first $|C|$ bits of Pad
$M \leftarrow Pad \oplus C$
return M

What is a secure encryption scheme?

- Recall, perfectly secure schemes are impractical
- We assume that adversaries are computationally bounded
- A scheme is secure when it is not insecure.
- Insecure = adversaries can do bad things.
- Bad things: an adversary, who sees ciphertexts
  - can compute the secret key
  - can compute some plaintexts
  - can compute the first bit of a plaintext
  - can compute the sum of the bits of a plaintext
  - can see when equal messages are encrypted
  - can compute ....

So what is a secure encryption scheme?

- Informally, an encryption scheme is secure if no adversary with "reasonable" resources who sees several ciphertexts can compute any* partial information about the plaintexts, besides some a-priori information.

* Any information, except the length of the plaintexts. We assume the length of the plaintexts is public.

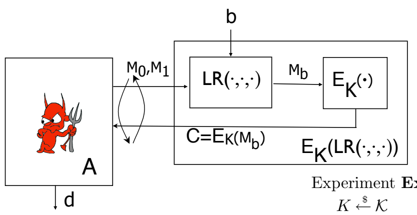
- Note, that the above implies that the bad things we mentioned do not happen. And the other "bad" things.
- While the above "definition" captures the right intuition, it's too informal to be useful.

Indistinguishability under chosen-plaintext attacks

Fix *SE*=(KeySp,E,D)

$K \xleftarrow{\$} \text{KeySp}$

For an adversary A and a bit b consider an experiment $\mathbf{Exp}_{\mathcal{SE}}^{\text{ind-cpa-b}}(A)$



The experiment returns d

Experiment $\mathbf{Exp}_{\mathcal{SE}}^{\text{ind-cpa-1}}(A)$
$K \xleftarrow{\$} \mathcal{K}$
$d \xleftarrow{\$} A^{\mathcal{E}_K(\text{LR}(\cdot,\cdot,1))}$
Return d

Experiment $\mathbf{Exp}_{\mathcal{SE}}^{\text{ind-cpa-0}}(A)$
$K \xleftarrow{\$} \mathcal{K}$
$d \xleftarrow{\$} A^{\mathcal{E}_K(\text{LR}(\cdot,\cdot,0))}$
Return d

The IND-CPA advantage of A is:

$$\mathbf{Adv}_{\mathcal{SE}}^{\text{ind-cpa}}(A) \;=\; \Pr\left[\mathbf{Exp}_{\mathcal{SE}}^{\text{ind-cpa-1}}(A)=1\right] - \Pr\left[\mathbf{Exp}_{\mathcal{SE}}^{\text{ind-cpa-0}}(A)=1\right]$$

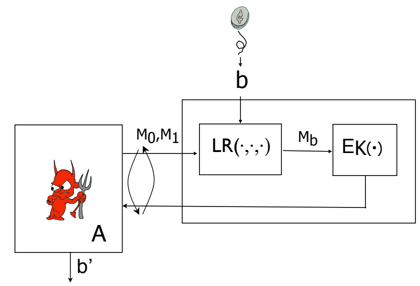
A symmetric encryption scheme *SE* is indistinguishable under chosen-plaintext attacks (IND-CPA secure) if for any adversary A with “reasonable” resources $\mathbf{Adv}_{\mathcal{SE}}^{\text{ind-cpa}}(A)$ is “small” (close to 0).

Alternative interpretation

Fix SE=(KeySp,E,D)

$K \xleftarrow{\$} \text{KeySp}$

For an adversary A consider an experiment $\mathbf{Exp}_{\mathcal{SE}}^{\text{ind-cpa-cg}}(A)$



Experiment $\mathbf{Exp}_{\mathcal{SE}}^{\text{ind-cpa-cg}}(A)$
$b \xleftarrow{\$} \{0,1\}$; $K \xleftarrow{\$} \mathcal{K}$
$b' \xleftarrow{\$} A^{\mathcal{E}_K(\text{LR}(\cdot,\cdot,b))}$
if $b=b'$ **then return** 1 **else return** 0

The experiment returns 1 iff A b’=b

<u>Claim.</u> $\mathbf{Adv}_{\mathcal{SE}}^{\text{ind-cpa}}(A) \;=\; 2\cdot\Pr\left[\mathbf{Exp}_{\mathcal{SE}}^{\text{ind-cpa-cg}}(A)=1\right]-1$

Proof of the claim

$$\begin{aligned}
&\Pr\left[\mathbf{Exp}_{\mathcal{SE}}^{\text{ind-cpa-cg}}(A)=1\right]\\
&= \Pr[b=b']\\
&= \Pr[b=b' \mid b=1]\cdot\Pr[b=1] + \Pr[b=b' \mid b=0]\cdot\Pr[b=0]\\
&= \Pr[b=b' \mid b=1]\cdot\frac{1}{2} + \Pr[b=b' \mid b=0]\cdot\frac{1}{2}\\
&= \Pr[b'=1 \mid b=1]\cdot\frac{1}{2} + \Pr[b'=0 \mid b=0]\cdot\frac{1}{2}\\
&= \Pr[b'=1 \mid b=1]\cdot\frac{1}{2} + (1-\Pr[b'=1 \mid b=0])\cdot\frac{1}{2}\\
&= \frac{1}{2}+\frac{1}{2}\cdot(\Pr[b'=1 \mid b=1]-\Pr[b'=1 \mid b=0])\\
&= \frac{1}{2}+\frac{1}{2}\cdot\left(\Pr\left[\mathbf{Exp}_{\mathcal{SE}}^{\text{ind-cpa-1}}(A)=1\right]-\Pr\left[\mathbf{Exp}_{\mathcal{SE}}^{\text{ind-cpa-0}}(A)=1\right]\right)\\
&= \frac{1}{2}+\frac{1}{2}\cdot\mathbf{Adv}_{\mathcal{SE}}^{\text{ind-cpa}}(A)
\end{aligned}$$

Why IND-CPA ensures that no partial information is leaked?

- Fix SE=(KeySp,E,D) with MsgSp=$\{0,1\}^m$. Assume there exists an adversary B that after seeing a few plaintexts-cipertexts pairs and a challenge ciphertext can compute the challenge plaintext. Namely, in
- Experiment $\mathbf{Exp}_{\mathcal{SE}}^{\text{pr-cpa}}(B)$
  $K \xleftarrow{\$} \mathcal{K}$
  $M' \xleftarrow{\$} \{0,1\}^m$
  $C \xleftarrow{\$} \mathcal{E}_K(M')$
  $M \xleftarrow{\$} B^{\mathcal{E}_K(\cdot)}(C)$
  If $M=M'$ **then return** 1 else return 0

$\mathbf{Adv}_{\mathcal{SE}}^{\text{pr-cpa}}(B) \;=\; \Pr\left[\mathbf{Exp}_{\mathcal{SE}}^{\text{pr-cpa}}(B)=1\right]$

is non-negligible

- Then SE is not IND-CPA secure.
- <u>Claim</u>. [IND-CPA⇒PR-CPA] Fix SE=(KeySp,E,D) with MsgSp=$\{0,1\}^m$. Then for every adversary B there exists an adversary A such that
- $\mathbf{Adv}_{\mathcal{SE}}^{\text{pr-cpa}}(B) \;\le\; \mathbf{Adv}_{\mathcal{SE}}^{\text{ind-cpa}}(A)+\frac{1}{2^m}$

and $q_A=q_B+1, \mu_A=\mu_B+m, t_A=t_B=O(\mu+m+c)$

- Proof. We define A as follows:

Adversary $A^{\mathcal{E}_K(\mathrm{LR}(\cdot,\cdot,b))}$
$M_0 \xleftarrow{\$} \{0,1\}^m$; $M_1 \xleftarrow{\$} \{0,1\}^m$
$C \leftarrow \mathcal{E}_K(\mathrm{LR}(M_0, M_1, b))$
Run adversary B on input C, replying to its oracle queries as follows
When B makes an oracle query X do
$Y \leftarrow \mathcal{E}_K(\mathrm{LR}(X, X, b))$
return Y to B as the answer
When B halts and outputs a plaintext M
If $M = M_1$ **then return** 1 else return 0

- We now analyze the adversary:

$$\Pr\left[\mathbf{Exp}^{\text{ind-cpa-1}}_{\mathcal{SE}}(A) = 1\right] \geq \mathbf{Adv}^{\text{pr-cpa}}_{\mathcal{SE}}(B)$$

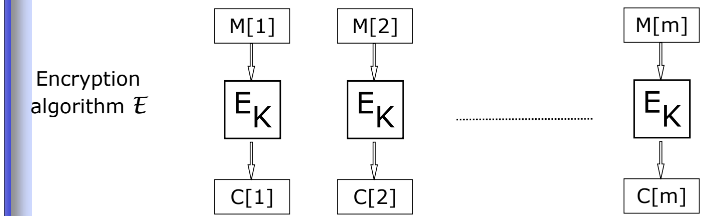
$$\Pr\left[\mathbf{Exp}^{\text{ind-cpa-0}}_{\mathcal{SE}}(A) = 1\right] \leq 2^{-m}$$

$$\begin{aligned}\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A) &= \Pr\left[\mathbf{Exp}^{\text{ind-cpa-1}}_{\mathcal{SE}}(A) = 1\right] - \Pr\left[\mathbf{Exp}^{\text{ind-cpa-0}}_{\mathcal{SE}}(A) = 1\right] \\ &\geq \mathbf{Adv}^{\text{pr-cpa}}_{\mathcal{SE}}(B) - 2^{-m} .\end{aligned}$$

The resources of A are justified by the description of A.

Analysis of the ECB mode.

Let $E:\{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. ECB=($\{0,1\}^k$,$\mathcal{E}$,$\mathcal{D}$):



Conjecture. ECB is PR-CPA secure.

Is ECB a good encryption scheme?

Is ECB IND-CPA secure?

ECB is not IND-CPA

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

$$\mathbf{Adv}^{ind-cpa}_{ECB}(A) = \Pr\left[\mathbf{Exp}^{ind-cpa-1}_{ECB}(A) = 1\right] - \Pr\left[\mathbf{Exp}^{ind-cpa-0}_{ECB}(A) = 1\right] = 1 - 0 = 1$$

- Claim. Any deterministic, stateless scheme is not IND-CPA
- Why?

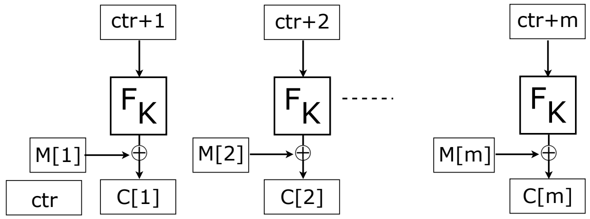
Analysis of the CTRC

Let F:{0,1}^{k}×{0,1}$^\ell$→{0,1}^{L} be a function family. CBC\$=({0,1}^{k},$\mathcal{E}$,$\mathcal{D}$):

Encryption algorithm $\mathcal{E}$

ctr is initially 0^ℓ

A current counter ctr is maintained as a state



The scheme is used to encrypt at most 2^ℓ blocks (so that the counter does not wrap around)

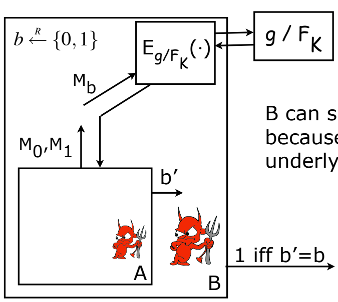
- How good is the scheme?
- The flaws seem hard to find.
- Q. But may be they exist and we just don't see them?
- A. The mode is as good as it can be and we can prove it.

Security of CTRC

- Theorem. For any adversary A there exists an adversary B such that
- $\mathbf{Adv}_{CTRC}^{ind-cpa}(A) \leq 2 \cdot \mathbf{Adv}_F^{prf}(B)$

  where $t_B = t_A + O(q_A + (l+L)\frac{\mu_A}{l}), q_B = \frac{\mu_A}{l}, \mu_B = \mu_A$
- Proof idea. We present an adversary B who needs to distinguish whether it is given an oracle access to a truly random function or an instance of F. B will use A's ability to break the CTRC encryption scheme. B will run A as a subroutine, simulating the ind-cpa experiment for it. B will answer A's oracle queries using its own oracle. Finally, if A wins, B will win.

- Proof. Let A be any "ind-cpa" adversary attacking CTRC. We present a "prf" adversary B:



g is a random instance of Func(ℓ,L)

B can simulate the CTRC encryption algorithm because it makes only "oracle" use of the underlying function F.

Adversary B^g
  $b \stackrel{\$}{\leftarrow} \{0,1\}$
  Run adversary A, replying to its oracle queries as follows
    When A makes an oracle query (M_0, M_1) do
      $C \stackrel{\$}{\leftarrow} \mathcal{E}_g(M_b)$
      Return C to A as the answer
    Until A stops and outputs a bit b'
  If $b' = b$ then return 1 else return 0

- Let us analyze B. Note that
- $\Pr\left[\mathbf{Exp}_F^{\text{prf-1}}(B)=1\right] = \Pr\left[\mathbf{Exp}_{\mathcal{SE}[F]}^{\text{ind-cpa-cg}}(A)=1\right] = \frac{1}{2}+\frac{1}{2}\cdot\mathbf{Adv}_{\mathcal{SE}[F]}^{\text{ind-cpa}}(A)$
- $\Pr\left[\mathbf{Exp}_F^{\text{prf-0}}(B)=1\right] = \Pr\left[\mathbf{Exp}_{\mathcal{SE}[\mathsf{Func}(\ell,L)]}^{\text{ind-cpa-cg}}(A)=1\right] = \frac{1}{2}+\frac{1}{2}\cdot\mathbf{Adv}_{\mathcal{SE}[\mathsf{Func}(\ell,L)]}^{\text{ind-cpa}}(A)$

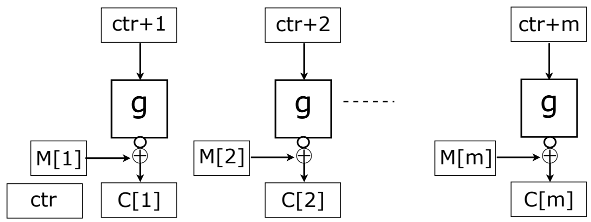
  and thus

$$\begin{aligned}\mathbf{Adv}_F^{\text{prf}}(B) &= \Pr\left[\mathbf{Exp}_F^{\text{prf-1}}(B)=1\right] - \Pr\left[\mathbf{Exp}_F^{\text{prf-0}}(B)=1\right] \\ &= \frac{1}{2}\cdot\mathbf{Adv}_{\mathcal{SE}[F]}^{\text{ind-cpa}}(A) - \frac{1}{2}\cdot\mathbf{Adv}_{\mathcal{SE}[\mathsf{Func}(\ell,L)]}^{\text{ind-cpa}}(A)\end{aligned}$$

We will show that $\mathbf{Adv}_{\mathcal{SE}[\mathsf{Func}(\ell,L)]}^{\text{ind-cpa}}(A) = 0$

and the statement of the theorem follows.Finally the resources of B are justified by the algorithm for B.

$\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}[\mathsf{Func}(\ell,L)]}(A) \;=\; 0$ because all the values corresponding to the red dots on the picture below are random and independent (since they are the results of a random function applied to distinct points) and thus C[1],…,C[m] are also random values, independent from the adversary A's challenge bit.

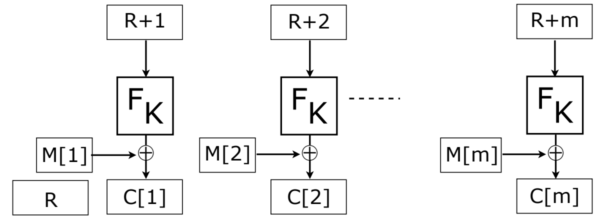


Analysis of the CTR$

Let F:{0,1}^{k}×{0,1}$^\ell$→{0,1}^{L} be a function family. CBC$=({0,1}^{k},$\mathcal{E}$,$\mathcal{D}$):

Encryption algorithm $\mathcal{E}$

$R \xleftarrow{\$} \{0,1\}^\ell$



Security of CTR$

- Theorem. For any adversary A there exists an adversary B such that
- $\mathbf{Adv}^{ind-cpa}_{CTR\$}(A) \leq 2 \cdot \mathbf{Adv}^{prf}_{F}(B) + \frac{\mu_A^2}{l^2 \cdot 2^l}$

  where $\quad t_B = t_A + O(q_A + (l+L)\frac{\mu_A}{l}), q_B = \frac{\mu_A}{l}, \mu_B = \mu_A$
-
- What does the security statement tell us?
  - Let F be AES, l=L=128. Assume one encrypts q=2^{30} messages, 1 Kb each (2^{13} bits), recall $\mathbf{Adv}^{prf}_{AES}(A) \leq\approx \frac{q_{AES}^2}{2^{128}}$
  - $\mathbf{Adv}^{ind-cpa}_{CTR\$}(A) \;\leq\; \approx 2 \cdot \frac{q_{AES}^2}{2^{128}} + \frac{\mu_A^2}{L^2 \cdot 2^l} = \frac{3 \cdot \mu^2}{L^2 \cdot 2^{128}}$
  - $\leq \frac{4 \cdot 2^{43 \cdot 2}}{128^2 \cdot 2^{128}} = \frac{1}{2^{54}}$
  -
  - Proof idea. As in the proof of the previous theorem.

- Proof. The adversary B is exactly like one in the proof of the previous theorem. But now we claim that
- $\mathbf{Adv}^{ind-cpa}_{CTR\$[Func(l,L)]}(A) \leq \frac{\mu_A^2}{2 \cdot l^2 \cdot 2^l}$
- Given this and the previous proof, the statement of the theorem follows.
- To prove the claim note that after q queries A made the inputs to the random function are

$$\begin{array}{llll} r_1+1, & r_1+2, & \cdots, & r_1+m_1 \\ r_2+1, & r_2+2, & \cdots, & r_2+m_2 \\ \vdots & & & \vdots \\ r_q+1, & r_q+2, & \cdots, & r_q+m_q \end{array}$$

Let NoCol be the event that these values are all distinct, and Col is the complement of NoCol. Then

$$\begin{aligned} &\mathbf{Adv}^{ind-cpa}_{CTR\$[Func(l,L)]}(A) \\ &= \Pr_1[A=1] - \Pr_0[A=1] \\ &= \Pr_1[A=1 \mid \mathsf{Col}] \cdot \Pr_1[\mathsf{Col}] + \Pr_1[A=1 \mid \mathsf{NoCol}] \cdot \Pr_1[\mathsf{NoCol}] \\ &\qquad - \Pr_0[A=1 \mid \mathsf{Col}] \cdot \Pr_0[\mathsf{Col}] - \Pr_0[A=1 \mid \mathsf{NoCol}] \cdot \Pr_0[\mathsf{NoCol}] \\ &= (\Pr_1[A=1 \mid \mathsf{Col}] - \Pr_0[A=1 \mid \mathsf{Col}]) \cdot \Pr_0[\mathsf{Col}] \\ &\leq \Pr_0[\mathsf{Col}]\ . \end{aligned}$$

- It remains to calculate $\Pr[\mathsf{Col}]$ (we drop the subscript 0 in the notation)

$$\begin{aligned}
\Pr[\mathsf{Col}] &= \Pr[\mathsf{Col}_q] \quad (\mathsf{Col}_i \text{ is the event that there is is collision in the first i rows}) \\
&= \Pr[\mathsf{Col}_{q-1}] + \Pr[\mathsf{Col}_q \mid \mathsf{NoCol}_{q-1}] \cdot \Pr[\mathsf{NoCol}_{q-1}] \\
&\leq \Pr[\mathsf{Col}_{q-1}] + \Pr[\mathsf{Col}_q \mid \mathsf{NoCol}_{q-1}] \\
&\leq \vdots \\
&\leq \Pr[\mathsf{Col}_1] + \sum_{i=2}^{q} \Pr[\mathsf{Col}_i \mid \mathsf{NoCol}_{i-1}] \\
&= \sum_{i=2}^{q} \Pr[\mathsf{Col}_i \mid \mathsf{NoCol}_{i-1}] \ .
\end{aligned}$$

$$\begin{aligned}
\Pr[\mathsf{Col}_i \mid \mathsf{NoCol}_{i-1}] &\leq \frac{(m_i + m_1 - 1) + (m_i + m_2 - 1) + \cdots + (m_i + m_{i-1} - 1)}{2^\ell} \\
&= \frac{(i-1)m_i + m_{i-1} + \cdots + m_1 - (i-1)}{2^\ell} \ ,
\end{aligned}$$

$$\begin{aligned}
\Pr[\mathsf{Col}] &\leq \sum_{i=2}^{q} \Pr[\mathsf{Col}_i \mid \mathsf{NoCol}_{i-1}] \\
&\leq \sum_{i=2}^{q} \frac{(i-1)m_i + m_{i-1} + \cdots + m_1}{2^\ell} \\
&= \frac{(q-1)(m_1 + \cdots + m_q)}{2^\ell} \ .
\end{aligned}$$

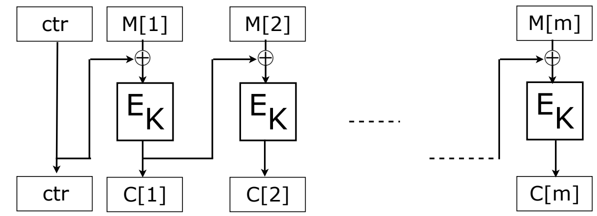
The statement follows after we note that $m_1 + \ldots + m_q = \mu_A / l$

Security of CBCC

Let E:{0,1}^{k}×{0,1}^{n}→{0,1}^{n} be a block cipher. CBCC=({0,1}^{k},$\mathcal{E}$,$\mathcal{D}$):

Stateful Encryption algorithm $\mathcal{E}$

ctr←0^n incremented for each new message



- Theorem. There exists an adversary A such that $\mathbf{Adv}^{ind-cpa}_{CBCC}(A) = 1$
- Proof idea. Adversary $A^{\mathcal{E}_K(\mathrm{LR}(\cdot,\cdot,b))}$

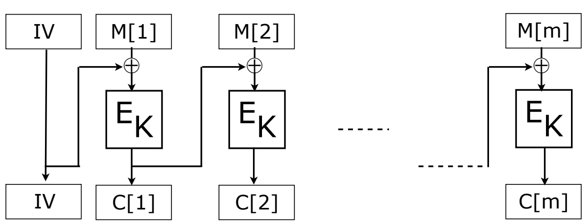
$$\begin{aligned}
&M_{0,1} \leftarrow 0^n \ ; \ M_{1,1} \leftarrow 0^n \\
&M_{0,2} \leftarrow 0^n \ ; \ M_{1,2} \leftarrow 0^{n-1}1 \\
&\langle \mathrm{IV}_1, C_1 \rangle \xleftarrow{\$} \mathcal{E}_K(\mathrm{LR}(M_{0,1}, M_{1,1}, b)) \\
&\langle \mathrm{IV}_2, C_2 \rangle \xleftarrow{\$} \mathcal{E}_K(\mathrm{LR}(M_{0,2}, M_{1,2}, b)) \\
&\text{If } C_1 = C_2 \ \textbf{then} \ \ \textbf{return} \ 1 \text{ else return } 0
\end{aligned}$$

Security of CBC$

Let E:{0,1}^{k}×{0,1}^{n}→{0,1}^{n} be a block cipher. CBC$=({0,1}^{k},$\mathcal{E}$,$\mathcal{D}$):

Encryption algorithm $\mathcal{E}$

IV←{0,1}^{n}



- Theorem. For any adversary A there exists an adversary B such that
- $\mathbf{Adv}^{ind-cpa}_{CBC\$}(A) \leq 2 \cdot \mathbf{Adv}^{prf}_{E}(B) + \frac{\mu_A^2}{n^2 \cdot 2^n}$

where $t_B = t_A + O(q_A + \mu_A), \ q_B = \frac{\mu_A}{n}, \ \mu_B = \mu_A$

Did we get all we wanted?

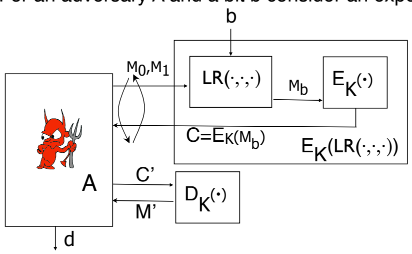
- Is IND-CPA security definition strong enough (does it take into account all the bad things that can happen?)
- An adversary wants to win: to get some partial information about the plaintext from a challenge ciphertext
- What if the adversary can make the receiver to decrypt other ciphertexts of the adversary's choice, learn the plaintexts and this helps it to win?
- Our definition didn't consider such "chosen-ciphertext" attacks

Indistinguishability under chosen-ciphertext attacks

Fix *SE*=(KeySp,E,D)

$K \xleftarrow{\$} \text{KeySp}$

For an adversary A and a bit b consider an experiment $\mathbf{Exp}^{ind-cca-b}_{\mathcal{SE}}(A)$



A is not allowed to query its decryption oracle on ciphertexts returned by its LR encryption oracle

The experiment returns d

The IND-CCA advantage of A is:

$$\mathbf{Adv}^{ind-cca}_{\mathcal{SE}}(A) = \Pr\left[\mathbf{Exp}^{ind-cca-1}_{\mathcal{SE}}(A)=1\right] - \Pr\left[\mathbf{Exp}^{ind-cca-0}_{\mathcal{SE}}(A)=1\right]$$

A symmetric encryption scheme *SE* is indistinguishable under chosen-ciphertext attacks (IND-CCA secure) if for any adversary A with "reasonable" resources $\mathbf{Adv}^{ind-cca}_{\mathcal{SE}}(A)$ is "small" (close to 0).