CS 276: Cryptography	Spring'06
Lecture 6 — February, 02	
Lecturer: David Wagner	*Scribe: Assane Gueye*

Symmetric Key Encryption

A symmetric key encryption scheme is given by:

- an encryption algorithm $E_K : keys \times Msg \rightarrow cyphertext$ that can be statefull and/or randomized
- a decryption algorithm $D_K : keys \times cyphertext \rightarrow Msg$ such that:
  correctness condition $\forall m \in Msg$, $D_K(E_K(m)) = m$

The correctness condition implies that the decryption algorithm cannot be statefull or randomized, because the same input cannot be decrypted into different messages.
Note that we consider messages of same length.

Let's now clarify the notion of computational security; for that we will give some "tentative" definitions.

Definition: Key protection
A scheme is secure if $Pr(A(M, C) = K) \leq \epsilon$, $\forall$ algo A running in time $\leq t$, where $C = E_K(M)$

Even though this definition gives a very small probability to recover the key from a given message and its corresponding cyphertext, it does not provide any protection for the message. For example an encryption algorithm of the kind $E_K(M) = M$ could be valid according to the definition but it is obvious but such an encryption algorithm is useless. In fact the definition is too "weak".
Let us consider another definition.

Definition: Message protection
A scheme is secure if $Pr(A(E_K(M)) = M) \leq \epsilon$, $\forall$ algo A running in time $\leq t$.

Again this definition protects the message from entire recovery but it is still has some weakness. For example $E_K(M) = lsb(M)| \ldots$ can be a valid encryption algorithm (for this definition), however it leaks some information about the message and that "some" information can be of very importance (e.g. it can be 'buy' or 'not buy' in the stocks market).
These two definitions fix some necessary conditions for security(key and message protection), but they were found to be not sufficient.
Let us now consider the problem a bit more formally.

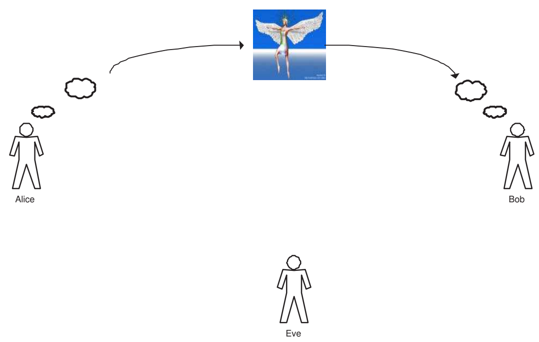

Figure 6.1. "Angelic" channel: an idealized world

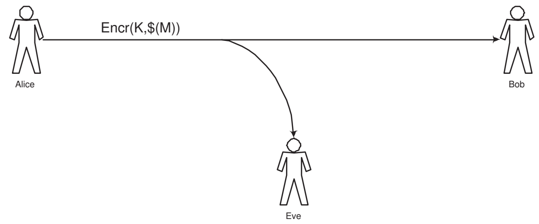

Figure 6.2. Idealized world: Alice encrypts a random message of same length as M

Say that Alice would like to send a message to Bob using a symmetric key scheme over an insecure channel. Eve (an eavesdropper) sits in between Alice and Bob and is trying to guess the message. The goal for Alice is to send the message in a way such that Eve would not be able to do better than just making a guess to recover the message.

In an idealized world, Alice would like to be able to just "think" the message and an "Angel" will carry it to Bob (Fig 6.1). In that way Eve would ignore everything about the message (at best Eve will know that a message of a given length has been sent).

The "angelic channel" is equivalent to the channel depicted in Fig 6.2 where Alice encrypts a random string of same length as the original message.

Now let's compare this last scheme to the real world where Alice has to encrypt the message to be sent (Fig 6.3).

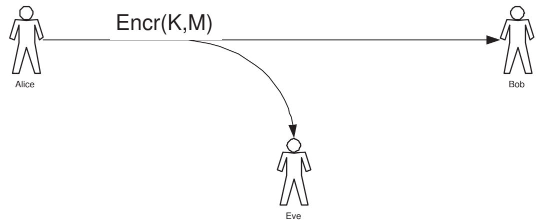

Figure 6.3. Real-world channel: Alice sends an encrypted version of the message

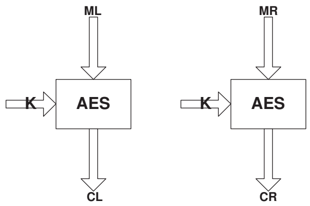

Figure 6.4. ECB mode

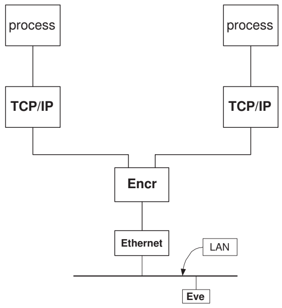

Figure 6.5. Multiuser system that uses a symmetric Key scheme to encode IP messages

Definition: An algorithm A is said to be $(t, q,)$-*real-or-random secure* if $Adv(A) \leq \epsilon$, $\forall A$ running in time $\leq t$, q queries, where

$$Adv(A) = |Pr(A^{E_K(.)} = 1) - Pr(A^{E_K(\$(.))} = 1)|$$

Let us consider now consider some examples.

Example: ECB-mode (Fig 6.4)
Claim: ECB-mode is not secure

Attack:

1. Encrypt $0^{128}||0^{128}$
2. If same output($C_L = C_R$), then output "real world"
   else output "ideal world"

Note that this attack can break any stateless and deterministic encryption algorithm.

Example: A practical system (Fig 6.5)
We consider a multiuser machine that use a symmetric key scheme to encrypt IP packets.

The same key is used to encrypt all users. Such a system can be vulnerable to known text attack. Security is achieved is IP packets do not provide any information about the message. If the encryption algorithm is real-or-random secure, the system will be secure.

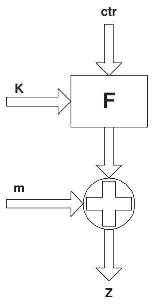

Figure 6.6. CTR mode

Example: CTR MODE (Fig 6.6)
The encryption and decryption algorithms for CTR MODE are given in table 6.1. F is define as $F : keys \times Ctrs \to 0, 1^{128}$.

$Encr = CTRC[F_K].\mathcal{E}$	$Decr = CTRC[F_K].\mathcal{D}$
static int c=0	
$Encr\{m\}$	$Decr\{i,Z\}$
1. $c \leftarrow +1$	1. return $F_K(i) \oplus Z$
2. return $(c, F_K(c) \oplus m)$	

Table 6.1. CTR mode encryption and decryption algorithms

The encryption algorithm is statefull: the transmitted message is $C = (ctr, Z)$.

Theorem 6.1. *If F is a secure PRF, then the CTR scheme is secure.*

For the proof we will use the following theorem.

Theorem 6.2. *Let R, $R : Ctrs \to 0, 1^{128}$, be a random function.*
CTRC[R] is $(\infty, |Ctrs|, 0)$-real-or-random secure.

Proof: Let A be any adversary, then $Adv(A) = |Pr(A^{CTRC[R].\mathcal{E}} = 1) - Pr(A^{CTRC[R].\mathcal{E}\circ\$} = 1)|$; where $\mathcal{E} \circ \$$ is the encryption of a random message drawn uniformly from the set of message of a given length.
On query m we have $(ctr, R(ctr) \oplus m) \equiv (ctr, uniform)$, because for every new value of ctr, $R(ctr)$ is uniformly drawn.
But in the *idealized world* we also have that $(ctr, R(ctr) \oplus \$m) \equiv (ctr, uniform)$ by definition.
So we have $(ctr, R(ctr) \oplus \$m) \equiv (ctr, R(ctr) \oplus m$, and thus $Adv(A) = 0$.
To proof theorem 6.1, we just replace R by a PRF F. $\square$

Theorem 6.3. *If F is a $(t, q, \epsilon) - PRF$ then $CRTC[F_K]$ is $(t - \mathcal{O}(q), min(q, |Ctrs|, 2\epsilon)$ real-or-random secure.*

Proof: Fix an adversary A.
Define new adversaries $B^f = A^{CRTR[f].\mathcal{E}}$ and $C^f = A^{CRTR[f].\mathcal{E}\oplus\$}$. We have $Pr(A^{CRTR[F_K].\mathcal{E}} = 1) = Pr(B^{F_K} = 1)$ and $Pr(A^{CRTR[F_K].\mathcal{E}\oplus\$} = 1) = Pr(C^{F_K} = 1)$.
Since F_K is a PRF we also have that $|Pr(B^{F_K} = 1) - Pr(B^R = 1)| \leq \epsilon$ and $|Pr(C^{F_K} = 1) - Pr(C^R = 1)| \leq \epsilon$.
Also since R is a random function we have:
$Pr(B^R = 1) = Pr(A^{CRTR[R].\mathcal{E}} = 1) = Pr(A^{CRTR[R].\mathcal{E}\oplus\$} = 1) = Pr(C^R = 1)$.
Thus

$$\begin{aligned}
Adv(A) &= |Pr(A^{CTRC[F_K].\mathcal{E}} = 1) - Pr(A^{CTRC[F_K].\mathcal{E}\circ\$} = 1)| \\
&= |Pr(B^{F_K} = 1) - Pr(C^{F_K} = 1)| \\
&= |Pr(B^{F_K} = 1) - Pr(B^R = 1) + Pr(C^R = 1) - Pr(C^{F_K} = 1)| \\
&\leq |Pr(B^{F_K} = 1) - Pr(B^R = 1)| + |Pr(C^R = 1) - Pr(C^{F_K} = 1)| \\
&\leq 2\epsilon
\end{aligned}$$

□

Now we can instantiate $F_K = AES$.
Conjecture: AES is a $(t, q, \frac{t}{2^{128}} + \frac{q^2}{2^{128}})$ secure PRF.
For example if the adversary has a power of$q = 2^{40}$ queries and $t = 2^{80}$ time units, the security level of $CTRC[AES]$ is $(2^{80}, 2^{40}, \frac{3}{2^{48}})$