Alin Tomescu, CSE408
Thursday, February 24th, Lecture #8

CBC mode security proof and Message Integrity

Theorem: If F_k is a (t,q,ε)-secure PRP then CBC^{F_k} (CBC mode with a random IV for each message) is a $\left(t - O(q), q, \varepsilon + \frac{q^2}{2^{n+1}}\right)$-RoR-secure encryption scheme.

Proof: We want to prove that $CBC^{F_k} \sim CBC^{F_k} \circ \$$. Let us define a variable x_i.

$$x_1 = IV\ XOR\ p_1$$

$$x_i = c_{i-1}\ XOR\ p_i, \forall i > 1$$

Note the following equality is true:

$$CBC^{F_k} \circ \$ = CBC^{F_k \circ \$}$$

Also note that since $F_k \underset{\varepsilon}{\overset{t,q}{\sim}} \pi$ then by DPI:

$$CBC^{F_k} \underset{\varepsilon}{\overset{t-O(q),q}{\sim}} CBC^{\pi}$$

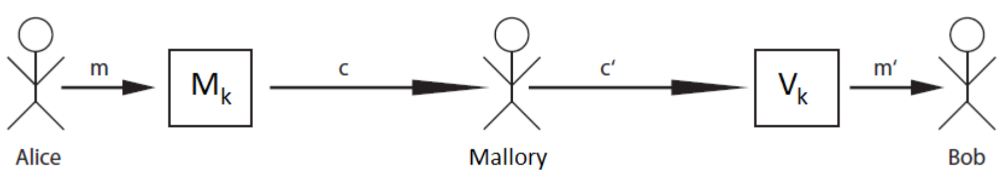
Also, we can reason that CBC^{π} and $CBC^{F_k \circ \$}$ are indistinguishable without collisions among the x_i's.

$$CBC^{\pi} \underset{q^2/2^{n+1}}{\overset{\infty,q}{\sim}} CBC^{F_k \circ \$}$$

Message integrity

First of all, encryption does not give you integrity. Encryption gives you secrecy. To get integrity, more work has to be done.

Our world:



- Alice sends messages to Bob and Mallory is in between them
- Alice encodes the message m as $c = M_k(m)$
- Mallory can see c, and can modify c into c' and send it to Bob
- Mallory can choose the m's and see the corresponding c's
- Bob will always runs $V_k(c') = m', \perp$
    - If $\perp$ is set, this tells Bob if c has been tampered with
    - $V_k(M_k(m)) = m, \forall m, k$
- Mallory gets access to the verification function V_k

There are **two levels of security** here: We can choose not to care if c is tampered as long as Bob still gets the original m, or we can choose to always be able to detect any tampering whatsoever.

Integrity of ciphertext (INT-CCA)

Mallory wins if after making q queries $m_1 \dots m_q$, which get mapped to $c_1 \dots c_q$, he finally manages to make a V_k query $c \notin \{c_1 \dots c_q\}$ such that $V_k(c) \neq \perp$

Definition: M_k, V_k is a (t, q, q', ε)-secure message integrity code if ∀ algorithms A running in time ≤ t and making $\leq q$ M_k queries and $\leq q'$ V_k queries then:

$$Adv\ A = \Pr[A^{M_k,V_k}\ wins] \leq \varepsilon$$

Winning, in this case, means successfully forging a message.