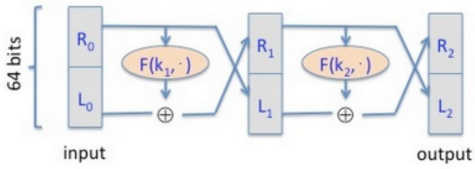
TD 2

Tuesday 30 September 2025 10:30

Problem 1 ***Two-Round Feistel Network***

Let $\mathbf{F}\colon \mathcal{K} \times \{0,1\}^{32} \to \{0,1\}^{32}$ be a secure PRF.
Recall that the Luby-Rackoff theorem states that a 3-round Feistel network gives a secure block cipher whenever a secure PRF F is used in its construction.
In contrast, a two-round construction has some undesired properties as we show next.



Assume that you observe two sequences c_1 and c_2. Design an adversary that can detect whether the two sequences have been generated by a purely random permutation or whether they have been obtained by encrypting the two messages $m_1 = [0^{32}||1^{32}]$ and $m_2 = [0^{32}||0^{32}]$ using above Feistel network.

For a 2-round Feistel network

$L_1 = R_0 \quad R_1 = F(K_1, R_0) \oplus L_0 \triangleq F_1(R_0) \oplus L_0$

$L_2 = R_1 \quad R_2 = F(K_2, R_1) \oplus L_1 \triangleq F_2(L_2) \oplus R_0$

$\Rightarrow L_0 \oplus L_2 = F_1(R_0)$ (1)

It makes more sense to flip the left part.

Suppose m_1 has $L_0' = 1^{32}$ $R_0' = 0^{32}$

m_2 has $L_0^2 = 0^{32}$ $R_0^2 = 0^{32}$

We therefore have $F_1(R_0') = F_1(R_0^2)$

but $L_0' = \overline{L_0^2}$

with (1), it must have $L_2' = \overline{L_2^2}$

For the attack, we define

$$A = \begin{cases} 1, & \text{if } L_2' = \overline{L_2^2} \\ 0, & \text{else} \end{cases}$$

$P(A=1 \mid m_1, m_2) = 1$, $P(A=1 \mid R_1, R_2) = 2^{-32}$

$Adv_A = 1 - 2^{-32}$, not negligible

Problem 2 ***CBC and Random CTR Mode Securitu***

Prove the following two statements:

1. Consider a positive integer $L > 0$ and a secure PRP $\mathbf{E}(\cdot,\cdot)$ over $\mathcal{X}$. Show that the L-block CBC construction with $\mathbf{E}$ is semantically secure against a q-query CPA if $\frac{q^2L^2}{|\mathcal{X}|}$ is negligible.
2. Consider a positive integer $L > 0$ and a secure PRF $\mathbf{F}(\cdot,\cdot)$ over $\mathcal{X}$. Show that the L-block Randomized Counter Mode construction with $\mathbf{F}$ is semantically secure against a q-query CPA if $\frac{q^2L}{|\mathcal{X}|}$ is negligible.

1. Suppose 3 systems:

S_0 the original system

S_1 the system with $E(\cdot,\cdot)$ replaced by a truly random P_R (used for all queries)

S_2 a perfectly secure OTP system

by def. → $P_0(1,1)$ for simplicity

$$Adv_{q\text{-}CAP} = |P_{S_0}(A=1 \mid b=1) - P_{S_0}(A=1 \mid B=0)|$$

$$= P_0(1,1) - P_1(1,1) + P_1(1,1) - P_2(1,1) + P_2(1,1) - P_0(1,0) + P_1(1,0) - P_1(1,0) + P_2(1,0) - P_2(1,0)$$

$$\leq |P_0(1,1) - P_1(1,1)| + |P_1(1,1) - P_2(1,1)| + |P_2(1,1) - P_2(1,0)| + |P_1(1,0) - P_0(1,0)| + |P_2(1,0) - P_1(1,0)|$$

$P_2(1,1) - P_2(1,0) = 0$ Since system 2 is perfect

$|P_0(1,1) - P_1(1,1)| = |P_1(1,0) - P_0(1,0)|$

is the advantage A has on S_0 over S_1 and is $\leq Adv_{PRP}$

Now compare system 1 and 2

Suppose for each query i, block j the input to P_R is

$X_{i,j} = m_{i,j} \oplus C_{i,j-1}$, with $C_{i,0} = IV$

The only possible way to distinguish between S_1 and S_2 is to have the event $C: X_{i,j} = X_{m,n}$ where $(i,j) \neq (m,n)$

Therefore $|P_2(1,0) - P_1(1,0)| = |P_1(1,1) - P_2(1,1)|$

$\leq P(C)$

$P(C) = P\left(\bigcup_{1 \leq i < j \leq N} X_i = X_j\right) \leq \sum_{1 \leq i < j \leq N} P(X_i = X_j)$

with $N = q \cdot 2$

$P(C) \leq \binom{N}{2} \frac{1}{|X|} = \frac{N(N-1)}{2|X|} = \frac{q^2 l^2}{2|X|}$

$\Rightarrow Adv_{q\text{-}CAP} \leq Adv_{PRP} + \frac{q^2 l^2}{2|X|} + 0$

$+ Adv_{PRP} + \frac{q^2 l^2}{2|X|}$

$= \underbrace{2 Adv_{PRP}}_{\text{negligible}} + q^2 l^2 / |X|$

2. Similarly, suppose

S_0 the original system

S_1 the system with $F(\cdot,\cdot)$ replaced by a truly random P_R (used for all queries)

S_2 a perfectly secure OTP system

Again the advantage A has on S_0 over S_1

$|P[A \text{ wins in } S_0] - P[A \text{ wins in } S_1]| \leq Adv_{PRF}$

Comparing between S_1 & S_2

Suppose for i-th query, j-th block

the random function gives

$S_{i,j} = P_R(IV_i + j)$

if all $S_{i,j}$ are distinct,

$C_{ij} = m_{ij} \oplus S_{i,j}$ is equivalent to OTP encryption

So the advantage A has on S_1 over S_2 exists on the collision

$|P[A \text{ wins in } S_1] - P[A \text{ wins in } S_2]| \leq P(C)$

$|P(A \text{ wins in } S_1) - P(A \text{ wins in } S_2)| \leq P(C)$
with event C: $V_{i+j} = V_{m+n}$ $(i,j) \neq (m,n)$
and again $P(C) \leq q^2L^2/2|X|$

Therefore, if we expand the advantage as we did in question 1. we would get
$Adv_A \leq 2Adv_{PRF} + q^2L^2/|X|$

Problem 3 ***Derived MACs***

Let $(\mathbf{S}, \mathbf{V})$ be a secure MAC defined over a message space $\mathcal{M} = \{0,1\}^n$, a tag space $\{0,1\}^{128}$, and a key space $\{0,1\}^\lambda$.
Which of the following derivates $(\mathbf{S}', \mathbf{V}')$ is a secure MAC:

1.
$$\mathbf{S}'(k,m) = \begin{cases} \mathbf{S}(k,[1\cdots1]), & \text{if } m = [0\cdots0] \\ \mathbf{S}(k,m) & \text{otherwise} \end{cases}$$
and
$$\mathbf{V}'(k,m,t) = \begin{cases} \mathbf{V}(k,[1\cdots1],t), & \text{if } m = [0\cdots0] \\ \mathbf{V}(k,m,t) & \text{otherwise} \end{cases}.$$

Not secure.
Suppose the adversary queries $m=[0\ldots0]$ and gets the tag t. It can forge a pair (m',t') with $m'=[1\ldots1]$, $t'=t$ and $Adv(A)=1$ since the tag for $[0\ldots0]$ is identical to the one for $[1\ldots1]$

2.
$$\mathbf{S}'(k,m) = \mathbf{S}(k, m \oplus [1\cdots1])$$
and
$$\mathbf{V}'(k,m,t) = \mathbf{V}(k, m \oplus [1\cdots1], t)$$

Secure
XOR with $[1\cdots1]$ is equivalent to bitwise inversion. The advantage of an efficient adversary remains the same since there is no extra information introduced.

3.
$$\mathbf{S}'(k,m) = \mathbf{S}(k,m)$$

and

$$\mathbf{V}'(k, m, t) = (\mathbf{V}(k, m, t) \text{ “or” } \mathbf{V}(k, m \oplus [1 \cdots 1], t)),$$

where “or” here denotes the logic or operation that returns ‘yes’ if and only if *one of the two sides returns ‘yes’.*

Not secure

The adversary A queries for m and gets t.

Then A could send $(\bar{m}, t)$ with

$$Adv_A = P(V(k, \bar{m}, t) = \text{“yes”})$$
$$= P(V(k, m \oplus [1 \cdots 1], t) = \text{“yes”})$$
$$= 1$$

$\bar{m}$ denotes bitwise inversion

4.

$$\mathbf{S}'((k_1, k_2), m) = (\mathbf{S}(k_1, m), \mathbf{S}(k_2, m))$$

and

$$\mathbf{V}'((k_1, k_2), m, (t_1, t_2)) = (\mathbf{V}(k_1, m, t_1), \mathbf{V}(k_2, m, t_2))$$

Secure Suppose adversary against s' is A

there exists adversaries B_1, B_2 against S

For A, it queries m and gets t_1, t_2

Let B_i query m and get t_i, $i = 1$ or 2 respectively

$Adv_A \leq Adv(B_1) + Adv(B_2)$

Since the event “A forges successfully”

is equivalent to “At least one of B_1 & B_2 succeeds”

we know that $Adv(B_1)$ or $Adv(B_2)$

is negligible. thus Adv_A is negligible.

Problem 4 ***One-Time and Manytime MAC***

Let $(\mathbf{S}, \mathbf{V})$ be a secure *one-time MAC*[1] with tag size $\{0,1\}^n$ and $\mathbf{F}$ a secure PRF onto $\{0,1\}^n$. Consider the Carter-Wegman construction to construct a new MAC:

$$\mathbf{S}_{\text{CW}}((k_1, k_2), m) = (r, \mathbf{F}(k_1, r) \oplus \mathbf{S}(k_2, m)),$$

where r is a randomness over $\{0,1\}^n$ and is freshly chosen at each application of the MAC.
The advantage of the Carter-Wegman MAC is that very fast implementations of one-time MACs $(\mathbf{S}, \mathbf{V})$ are known and that the PRF $\mathbf{F}$ (which might be more complex) has to be calculated only for a short input.

1. Find a valid verification algorithm $\mathbf{V}_{\text{CW}}$ for above MAC encoding function $\mathbf{S}_{\text{CW}}$.
2. Argue that the Carter-Wegman MAC $(\mathbf{S}_{\text{CW}}, \mathbf{V}_{\text{CW}})$ is secure even with multiple queries $q > 1$. (At each query a different randomness will be used to generate the tag.)

1. denote $t_1 = Scw[1] = r$

$t_2 = Scw[2] = F(k_1, r) \oplus S(k_2, m)$

$V(t_1, t_2, k_1, k_2, m) =$

$\mathbb{1}\{F(k_1, t_1) \oplus S(k_2, m) = t_2\}$

2. Suppose we have another system S_1 where $F(k_1, r)$ is replaced by a truly randomness

Since $F()$ is supposed to be secure

$Adv_A(S_0) - Adv_A(S_1) \leq \varepsilon$ negligible

For the new system, the adversary A queries q times and gets

$(r_i, S(k_2, m_i) \oplus R(r_i))$

For a forgery, A generates $(\tilde{m}, \tilde{t}_1, \tilde{t}_2)$

Case 1: if $\tilde{t}_1$ is different from r_i, $\forall i = 1 \ldots q$

$P(\tilde{t}_2 = S(k_2, \tilde{m}) \oplus R(\tilde{t}_1)) = 2^{-n}$

due to the truly random function $R(\cdot)$

Case 2: if $\tilde{t}_1 = r_k$, $k = 1 \ldots q$

by def, $\tilde{m} \neq m_k$

The adversary needs

$S(k_2, \tilde{m}) \oplus R(r_k) = \tilde{t}_2$

with knoledge

$S(k_2, m_k) \oplus R(r_k) = t_{2k}$

The advantage it has is exactly the one it would have on the one-time MAC.

Suppose $Adv_A((S, V)) = \varepsilon$

Then $Adv_A((S^{cw}, V^{cw})) = 2^{-n} + \varepsilon$