6.1 (The 802.11b insecure MAC). Consider the following MAC (a variant of this was used for WiFi encryption in 802.11b WEP). Let F be a PRF defined over $(\mathcal{K}, \mathcal{R}, \mathcal{X})$ where $\mathcal{X} := \{0,1\}^{32}$. Let CRC32 be a simple and popular error-detecting code meant to detect random errors; CRC32(m) takes inputs $m \in \{0,1\}^{\leq \ell}$ and always outputs a 32-bit string. For this exercise, the only fact you need to know is that CRC32$(m_1) \oplus$ CRC32$(m_2) =$ CRC32$(m_1 \oplus m_2)$. Define the following MAC system (S, V):

only 32 bits

$$S(k,m) := \{\ r \xleftarrow{R} \mathcal{R},\ t \leftarrow F(k,r) \oplus \text{CRC32}(m),\ \text{output } (r,t)\ \}$$
$$V(k,m,(r,t)) := \{\ \text{accept if } t = F(k,r) \oplus \text{CRC32}(m) \text{ and reject otherwise}\}$$

Show that this MAC system is insecure.

idea: existential forgery?

(m_1, t_1), (m_2, t_2)

$t_1 = F(k, r_1) \oplus CRC32(m_1)$

$t_2 = F(k, r_2) \oplus CRC32(m_2)$

$m_3 = m_1 \oplus m_2$?

$t_3 = F(k, r_3) \oplus CRC32(m_1 \oplus m_2)$

$= F(k, r_3) \oplus CRC32(m_1) \oplus CRC32(m_2)$

with $\sqrt{|\mathcal{X}|}$ queries, $P(\exists\, t_1 = t_2 \text{ for } m_1 \neq m_2) \geq 1/2$

$MACadv[A, I] = PRF[B, F] + P(\text{collision})$

$\leq \frac{1}{|\mathcal{X}|} + \varepsilon$

$\Rightarrow$ with 2^{16} queries.

$MACadv[A, I] \geq \frac{1}{2^{32}} + \frac{1}{2}$

Lesson: MAC tag space has to be big enough, or else the key has to be frequently updated.

6.2 (Tighter bounds with verification queries). Let F be a PRF defined over $(\mathcal{K}, \mathcal{X}, \mathcal{Y})$, and let $\mathcal{I}$ be the MAC system derived from F, as discussed in Section 6.3. Let $\mathcal{A}$ be an adversary that attacks $\mathcal{I}$ as in Attack Game 6.2, and which makes at most Q_{v} verification queries and at most Q_{s} signing queries. Theorem 6.1 says that there exists a Q_{s}-query MAC adversary $\mathcal{B}$ that attacks $\mathcal{I}$ as in Attack Game 6.1, where $\mathcal{B}$ is an elementary wrapper around $\mathcal{A}$, such that $\mathrm{MAC}^{\mathrm{vq}}\mathsf{adv}[\mathcal{A}, \mathcal{I}] \leq \mathrm{MACadv}[\mathcal{B}, \mathcal{I}] \cdot Q_{\mathrm{v}}$. Theorem 6.2 says that there exists a $(Q_{\mathrm{s}} + 1)$-query PRF adversary $\mathcal{B}'$ that attacks F as in Attack Game 4.2, where $\mathcal{B}'$ is an elementary wrapper around $\mathcal{B}$, such that $\mathrm{MACadv}[\mathcal{B}, \mathcal{I}] \leq \mathrm{PRFadv}[\mathcal{B}', F] + 1/|\mathcal{Y}|$. Putting these two statements together, we get

$$\mathrm{MAC}^{\mathrm{vq}}\mathsf{adv}[\mathcal{A}, \mathcal{I}] \leq (\mathrm{PRFadv}[\mathcal{B}', F] + 1/|\mathcal{Y}|) \cdot Q_{\mathrm{v}}$$

This bound is not the best possible. Give a direct analysis that shows that there exists a $(Q_{\mathrm{s}} + Q_{\mathrm{v}})$-query PRF adversary $\mathcal{B}''$, where $\mathcal{B}''$ is an elementary wrapper around $\mathcal{A}$, such that

$$\mathrm{MAC}^{\mathrm{vq}}\mathsf{adv}[\mathcal{A}, \mathcal{I}] \leq \mathrm{PRFadv}[\mathcal{B}'', F] + Q_{\mathrm{v}}/|\mathcal{Y}|.$$

idea:

$$\mathrm{MAC}^{vq}\mathrm{adv}[\mathcal{A}, \mathcal{I}] \leq \mathrm{MACadv}[\mathcal{B}, \mathcal{I}] \cdot Q_v$$

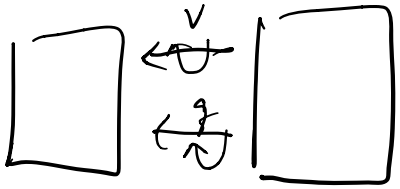
$$\mathrm{MACadv}[\mathcal{A}, \mathcal{I}] \leq \mathrm{PRFadv}[\mathcal{B}', F] + \frac{1}{|\mathcal{Y}|}$$

NOTES: ← all MAC on relatively short inputs.

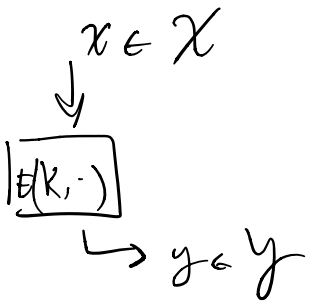
$$\rightarrow \mathrm{MAC}^{vq}\mathrm{adv}[\mathcal{A}, \mathcal{I}] \leq \left(\mathrm{PRFadv}[\mathcal{B}', F] + \frac{1}{|\mathcal{Y}|}\right) \cdot Q_v$$

Prove: $\mathrm{PRFadv}[\mathcal{B}'', F] + \frac{Q_v}{|\mathcal{Y}|}$

Goal:



$\Longleftrightarrow$



NOTE: all queries are unique, $m_i \neq m_j$.

Proof: # Game 0: MAC (V.q) game.

$K \xleftarrow{R} \mathcal{K}$

Signing query:

$t_i \xleftarrow{R} F(K, m_i)$

Send $t_i \rightarrow \mathcal{A}$

Verification query:

$r_j \leftarrow V(K, \hat{m}_j, \hat{t}_j)$

Send $r_j \rightarrow \mathcal{A}$

W_0: for some j, r_j = accept

$$\Pr[W_0] = \mathrm{MAC}^{vq}\mathrm{adv}[\mathcal{A}, \mathcal{I}]$$

Game 1: PRF card game:

$f \xleftarrow{R} Funs[X, Y]$

$t_i \xleftarrow{R} f(K, m_i)$

$|Pr[W_1] - Pr[W_0]| = PRFadv[B, F]$

Next, directly bound $Pr[W_1]$, since f is a truly random function, for $m \notin \{m_0, m_1, \dots\}$, every verification query has $\frac{1}{|Y|}$ of prob of winning

$$\rightarrow Pr[W_1] \leq \frac{Q_v}{|Y|}$$

$$\Rightarrow Pr[W_0] \leq |Pr[W_0] - Pr[W_1]| + Pr[W_1]$$

$$= PRFadv[B', F] + \frac{Q_v}{|Y|}$$

supposedly no weaker than single-key ←

6.3 (Multi-key MAC security). Just as we did for semantically secure encryption in Exercise 5.2, we can extend the definition of a secure MAC from the single-key setting to the multi-key setting. In this exercise, you will show that security in the single-key setting implies security in the multi-key setting.

(a) Show how to generalize Attack Game 6.2 so that an attacker can submit both signing queries and verification queries with respect to several MAC keys $k_1, \ldots, k_Q$. At the beginning of the game the adversary outputs a number Q indicating the number of keys it wants to attack and the challenger chooses Q random keys $k_1, \ldots, k_Q$. Subsequently, every query from the attacker includes an index $j \in \{1, \ldots, Q\}$. The challenger uses the key k_j to respond to the query.

(b) Show that every efficient adversary $\mathcal{A}$ that wins your multi-key MAC attack game with probability ϵ can be transformed into an efficient adversary $\mathcal{B}$ that wins Attack Game 6.2 with probability ϵ/Q.

Hint: This is *not* done using a hybrid argument, but rather a "guessing" argument, somewhat analogous to that used in the proof of Theorem 6.1. Adversary $\mathcal{B}$ plays the role of challenger to adversary $\mathcal{A}$. Once $\mathcal{A}$ outputs a number Q, $\mathcal{B}$ chooses Q random keys $k_1, \ldots, k_Q$ and a random index $\omega \in \{1, \ldots, Q\}$. When $\mathcal{A}$ issues a query for key number $j \neq \omega$, adversary $\mathcal{B}$ uses its key k_j to answer the query. When $\mathcal{A}$ issues a query for the key k_ω, adversary $\mathcal{B}$ answers the query by querying its MAC challenger. If $\mathcal{A}$ outputs a forgery under key k_ω then $\mathcal{B}$ wins the MAC forgery game. Show that $\mathcal{B}$ wins Attack Game 6.2 with probability ϵ/Q. We call this style of argument "plug-and-pray:" $\mathcal{B}$ "plugs" the key he is challenged on at a random index ω and "prays" that $\mathcal{A}$ uses the key at index ω to form his existential forgery.

(a) Prove: $MAC^{vg}adv[\mathcal{A}, I] \longrightarrow MAC^{MK}adv[\mathcal{A}, I]$

chal adv

$k_1, \ldots k_Q \xleftarrow{R} K^Q$

m_i, k_i ←

$t_i = S(k_i, m_i)$ $\quad t_i \rightarrow$ $\cup Q_S$

$r_j = V(\hat{m_j}, \hat{t_j}, k_j)$ ← $\hat{m_j}, \hat{t_j}, k_j$

$r_j \rightarrow$ $\cup Q_V$

$MAC^{MK}adv[\mathcal{A}, I]$ defined as probability of having some r_j = accept.

(b) chal $\mathcal{B}$ obviously

$MACadv^{MK}[\mathcal{A}, \mathcal{E}] = Q \cdot MAC^{vg}[\mathcal{B}, \mathcal{E}]$

$\omega \in \{1, \ldots Q\}$ $\quad (t, v)$ ←

← if $i = \omega$ $\quad t_i \rightarrow$ MK adv. $\mathcal{A}$

otherwise $t \xleftarrow{R} T$ →

6.4 (Multicast MACs). Consider a scenario in which Alice wants to broadcast the same message to n users, $U_1, \ldots, U_n$. She wants the users to be able to authenticate that the message came from her, but she is not concerned about message secrecy. More generally, Alice may wish to broadcast a series of messages, but for this exercise, let us focus on just a single message.

(a) In the most trivial solution, Alice shares a MAC key k_i with each user U_i. When she broadcasts a message m, she appends tags $t_1, \ldots, t_n$ to the message, where t_i is a valid tag for m under key k_i. Using its shared key k_i, every user U_i can verify m's authenticity by verifying that t_i is a valid tag for m under k_i.

≤ (n-1) MACadv.

Assuming the MAC is secure, show that this broadcast authentication scheme is secure *even if users collude*. For example, users $U_1, \ldots, U_{n-1}$ may collude, sharing their keys $k_1, \ldots, k_{n-1}$ among each other, to try to make user U_n accept a message that is not authentic.

(b) While the above broadcast authentication scheme is secure, even in the presence of collusions, it is not very efficient; the number of keys and tags grows linearly in n.

Here is a more efficient scheme, but with a weaker security guarantee. We illustrate it with $n = 6$. The goal is to get by with $\ell < 6$ keys and tags. We will use just $\ell = 4$ keys, $k_1, \ldots, k_4$. Alice stores all four of these keys. There are $6 = \binom{4}{2}$ subsets of $\{1, \ldots, 4\}$ of size 2. Let us number these subsets $J_1, \ldots, J_6$. For each user U_i, if $J_i = \{v, w\}$, then this user stores keys k_v and k_w.

When Alice broadcasts a message m, she appends tags $t_1, \ldots, t_4$, corresponding to keys $k_1, \ldots, k_4$. User U_i verifies tags t_v and t_w, using its keys k_v, k_w, where $J_i = \{v, w\}$ as above.

Assuming the MAC is secure, show that this broadcast authentication scheme is secure *provided no two users collude*. For example, using the keys that he has, user U_1 may attempt to trick user U_6 into accepting an inauthentic message, but users U_1 and U_2 may not collude and share their keys in such an attempt.

(c) Show that the scheme presented in part (b) is completely insecure if two users are allowed to collude.

(b) Provided that no 2 users may collude, no parties could assemble the two keys that "victim" have. (i.e. at least one unique to yourself)

↳ as secure as single-key

(c) one assumption is broken, then it's as bad as key leakage.

↳ completely insecure

6.5 (MAC combiners). We want to build a MAC system $\mathcal{I}$ using two MAC systems $\mathcal{I}_1 = (S_1, V_1)$ and $\mathcal{I}_2 = (S_2, V_2)$, so that if at some time one of $\mathcal{I}_1$ or $\mathcal{I}_2$ is broken (but not both) then $\mathcal{I}$ is still secure. Put another way, we want to construct $\mathcal{I}$ from $\mathcal{I}_1$ and $\mathcal{I}_2$ such that $\mathcal{I}$ is secure if either $\mathcal{I}_1$ or $\mathcal{I}_2$ is secure.

∈ robustness at a higher cost.

(a) Define $\mathcal{I} = (S, V)$, where

$$S(\ (k_1, k_2),\ m) := (\ S_1(k_1, m),\ S_2(k_2, m)\ ),$$

and V is defined in the obvious way: on input $(k, m, (t_1, t_2))$, V accepts iff both $V_1(k_1, m, t_1)$ and $V_2(k_2, m, t_2)$ accept. Show that $\mathcal{I}$ is secure if either $\mathcal{I}_1$ or $\mathcal{I}_2$ is secure.

↳ if only I_1 is broken, Then $V_2(k_2, m, t_2)$ → reject

I_2 V_1 → reject

(b) Suppose that $\mathcal{I}_1$ and $\mathcal{I}_2$ are deterministic MAC systems (see the definition on page 214), and that both have tag space $\{0,1\}^n$. Define the deterministic MAC system $\mathcal{I} = (S, V)$, where

$$S(\ (k_1, k_2),\ m) := S_1(k_1, m) \oplus S_2(k_2, m).$$

Show that $\mathcal{I}$ is secure if either $\mathcal{I}_1$ or $\mathcal{I}_2$ is secure.

Proof: #game 0: Attack game 6.2.

$\Pr[W_0] = \mathrm{MAC}_{adv}[A, I]$

#game 1: k_1 is given to adversary.

$|\Pr[W_0] - \Pr[W_1]| = \mathrm{MAC}_{adv}[B_1, I_1]$

#game 2: k_2 are given to adv.

$|\Pr[W_2] - \Pr[W_1]| = \mathrm{MAC}_{adv}[B_2, I_2]$

now directly bound $\Pr[W_1]$ & $\Pr[W_1]$

$\Pr[W_1] \le \mathrm{MAC}_{adv}[B_1', I_2]$

$\Pr[W_2] \le \mathrm{MAC}_{adv}[B_2', I_1]$

$\Rightarrow |\mathrm{MAC}_{adv}[A, I]| \le \mathrm{MAC}_{adv}[B_1, I_1] + \mathrm{MAC}_{adv}[B_2, I_2]$

6.6 (Concrete attacks on CBC and cascade). We develop attacks on F_{CBC} and F^* as prefix-free PRFs to show that for both security degrades quadratically with number of queries Q that the attacker makes. For simplicity, let us develop the attack when inputs are exactly three blocks long.

(a) Let F be a PRF defined over $(\mathcal{K}, \mathcal{X}, \mathcal{X})$ where $\mathcal{X} = \{0,1\}^n$, where $|\mathcal{X}|$ is super-poly. Consider the F_{CBC} prefix-free PRF with input space $\mathcal{X}^3$. Suppose an adversary queries the challenger at points (x_1, y_1, z), (x_2, y_2, z), $\ldots (x_Q, y_Q, z)$, where the x_i's, the y_i's, and z are chosen randomly from $\mathcal{X}$. Show that if $Q \approx \sqrt{|\mathcal{X}|}$, the adversary can predict the PRF at a new point in $\mathcal{X}^3$ with probability at least 1/2.

(b) Show that a similar attack applies to the three-block cascade F^* prefix-free PRF built from a PRF defined over $(\mathcal{K}, \mathcal{X}, \mathcal{K})$. Assume $\mathcal{X} = \mathcal{K}$ and $|\mathcal{K}|$ is super-poly. After making $Q \approx \sqrt{|\mathcal{K}|}$ queries in $\mathcal{X}^3$, your adversary should be able to predict the PRF at a new point in $\mathcal{X}^3$ with probability at least 1/2.

Both questions are direct application of devising an adversary that leverages the "Birthday Paradox". thus please see Appendix for more basics.

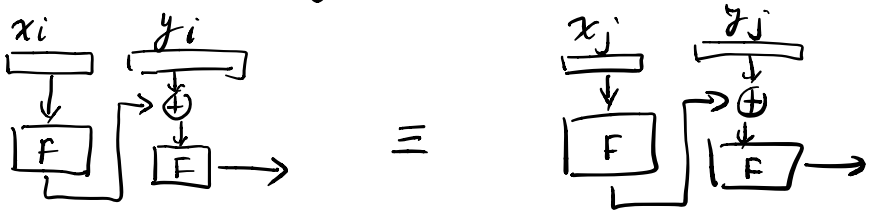
(a)

Proof Idea: (NOT 100% sure)

Since we already know that with $Q \approx \sqrt{|\mathcal{X}|}$ queries, there's $\approx 50\%$ chance of finding collisions (i.e. 2 points in $\mathcal{X}^3$ that result in the same tag). the key question to ask, therefore is "how to transform our collision finding advantage into predictability"?

if $F_{CBC}(k, (x_i, y_i, z)) = F_{CBC}(k, (x_j, y_j, z))$ $i \neq j$,

then



in the future, given (x_i, y_i, z_k) new tuple, the adversary could existentially forge another yet-queried valid tuple:

$$(x_j, y_j, z_k)$$

If the adversary didn't find any collision with Q queries, then gives random (msg, tag) tuple as its prediction.

(b) Similar to (a).

6.7 (Weakly secure MACs). It is natural to define a weaker notion of security for a MAC in which we make it harder for the adversary to win; specifically, in order to win, the adversary must submit a valid tag on a new message. One can modify the winning condition in Attack Games 6.1 and 6.2 to reflect this weaker security notion. In Attack Game 6.1, this means that to win, in addition to being a valid pair, the adversary's candidate forgery pair (m, t) must satisfy the constraint that m is not among the signing queries. In Attack Game 6.2, this means that the adversary wins if the challenger ever responds to a verification query $(\hat{m}_j, \hat{t}_j)$ with accept, where $\hat{m}_j$ is not among the signing queries made prior to this verification query. These two modified attack games correspond to notions of security that we call *weak security without verification queries* and *weak security with verification queries*. Unfortunately, the analog of Theorem 6.1 does not hold relative to these weak security notions. In this exercise, you are to show this by giving an explicit counter-example. Assume the existence of a secure PRF (defined over any convenient input, output, and key spaces, of your choosing). Show how to "sabotage" this PRF to obtain a MAC that is weakly secure without verification queries but is not weakly secure with verification queries.

Solution Idea:

to give counter example, it's crucial to ask:

1. why verification queries don't help in Attack Game 6.2?
2. what changed when we adopt "weakly secure MAC" notion?

When proving equivalence of Attak Game 6.1 & 6.2, we utilize an elementary wrapper $\mathcal{B}$ which randomly select 1 (msg, tag) pair out of all verification queries from $\mathcal{A}$ and output this pair to its challenger as a forgery. while returning REJECT to $\mathcal{A}$ for the rest of verification queries. let's refresh the key point in the proof.

Game 1. This is the same as Game 1, except that the line marked (∗) above is changed to:

send reject to $\mathcal{A}$

That is, when responding to a verification query, the challenger always responds to $\mathcal{A}$ with reject. We also define W_1 to be the event that in Game 1, r_j = accept for some j. Even though the challenger does not notify $\mathcal{A}$ that W_1 occurs, both Games 0 and 1 proceed identically until this event happens, and so events W_0 and W_1 are really the same; therefore,

$$\Pr[W_1] = \Pr[W_0]. \tag{6.2}$$

Also note that in Game 1, although the r_j values are used to define the winning condition, they are not used for any other purpose, and so do not influence the attack in any way.

NOTE: reason why $Pr[W_1] = Pr[W_0]$ is that: prob of $\mathcal{A}$ guessing a valid forgery pair for some j DOES NOT depends on or affected by "whether $\mathcal{A}$ actual know the verification query result".

↳ it's a fact, any Qv before the 1st correct one returns REJECT.

The key intuition..!

verification queries are as hard as winning the original MAC attack game.

↓

it doesn't hurt for adv. to play couple of more times.

→ Now, what changed?

For weakly secure MAC, verification query is more powerful, leaks more info than its restricted information game in MAC attack game.

Solution: