CMPT 404 — Cryptography and Protocols

Exercises on Message Authentication Schemes, CCA Security and Number Theory.
Due: Thursday, March 15th (at the beginning of the class)

1. Given $f : \{0,1\}^n \to \{0,1\}^n$, define $f' : \{0,1\}^{2n} \to \{0,1\}^{2n}$ as follows: for $x, r \in \{0,1\}^n$ define $f'(x \circ r) = f(x) \circ r$. (Where $\circ$ denotes concatenation.) Prove that if $f(\cdot)$ is a one-way permutation then so is $f'(\cdot)$.

2. Consider the following variant of CMA-security for MACs: instead of giving the adversary black boxes for both the signing and verification algorithms, give it only a black box for the signing algorithm. Let's call this definition CMA'-security. That is,

   > A pair of algorithms $(\mathsf{Sign}, \mathsf{Ver})$ (with $\mathsf{Sign} : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^t$, $\mathsf{Ver} : \{0,1\}^n \times \{0,1\}^m \times \{0,1\}^t \to \{0,1\}$) is a (T, ε)-CMA'-secure MAC if for every x, k, $\mathsf{Ver}_k(x, \mathsf{Sign}_k(x)) = 1$ and for every T-time Adv, if we run the following experiment:
   >
   > - Choose $k \longleftarrow \{0,1\}^n$
   > - Give adversary access to black box for $\mathsf{Sign}_k(\cdot)$
   > - Adversary *wins* if it comes up with a pair $\langle x', s' \rangle$ such that **(a)** x' is *not* one of the messages that the adversary gave to the black box $\mathsf{Sign}_k(\cdot)$ and **(b)** $\mathsf{Ver}_k(x', s') = 1$.
   >
   > Then the probability Adv wins is at most ε.
   >
   > $(\mathsf{Sign}, \mathsf{Ver})$ is CMA'-secure if there are super-polynomial functions T, ε such that for every n, $(\mathsf{Sign}, \mathsf{Ver})$ is $(T(n), \varepsilon(n))$-CMA'-secure. In other words, there is no polynomial-time Adv that succeeds with polynomial probability to break it.

   A MAC scheme has *unique tags* if for every message there is only one tag that passes verification. An equivalent way of stating this property is that the verification algorithm on input x and t outputs 1 if and only if $\mathsf{Sign}_k(x) = t$. Note that the MAC scheme we saw in class has this property. Prove that for MACs with unique tags, CMA security and CMA' security are *equivalent* (e.g., such a scheme is (T, ε)-CMA secure if and only if it is (T', ε')-CMA' secure for some T',ε' polynomially related to T, ε. (The condition of unique tags is important — if a MAC scheme does *not* have unique tags then these notions may not be equivalent.)

3. For each of the following statements either prove that it is true, or give a counterexample showing that it is false:[1]

   (a) A MAC tag always maintains secrecy of the message. That is, if $(\mathsf{Sign}, \mathsf{Ver})$ is a CMA-secure MAC with m-bit long messages and n-bit long keys, then for every two strings x and x' in $\{0,1\}^m$, the random variable $\mathsf{Sign}_{U_n}(x)$ is computationally indistinguishable from the random variable $\mathsf{Sign}_{U_n}(x')$.

[1] Counterexamples can be contrived as long as they are valid. That is, if a statement says that every MAC scheme satisfies a certain property then to show this statement false you can present *any* chosen-message attack secure MAC scheme that does not satisfy this property. The MAC scheme can be constructed just for the sake of a counterexample, and does not have to be "natural looking", as long as it is chosen-message attack secure.

(b) A MAC tag always has to be longer than the message. That is, for every MAC scheme $(\mathsf{Sign}, \mathsf{Ver})$, $|\mathsf{Sign}_k(x)| \geq |x|$.

(c) A CMA-secure MAC scheme has to be *probabilistic* that is, $\mathsf{Sign}_k(x)$ can't be a deterministic function of k and x and has to toss additional coins.

(d) (*optional*) Reusing a key for authentication and encryption does not harm secrecy: Suppose that $(\mathsf{Sign}, \mathsf{Ver})$ is a secure MAC with n bit key and (E, D) is a CPA-secure encryption scheme with n bit key. Suppose that a sender chooses $k \longleftarrow bits^n$ and a random number $x \longleftarrow 1, \ldots, 100$, computes $y = \mathsf{E}_k(x)$ and sends $y, \mathsf{Sign}_k(y)$ (note that the same key k is used for both authentication and encryption). Then, *secrecy* is preserved: an eavesdropper can not guess x with probability higher than, say 1/99.

(e) (*optional*) Reusing a key for authentication and encryption does not harm integrity: In the same setting as the previous item, *integrity* is preserved. That is, if the receiver obtains (y, t), where $\mathsf{Ver}_k(y, t) = 1$ and computes $x' = \mathsf{D}_k(y)$ then $x = x'$.

4. Consider the following hash function. Let E be a block cipher. Then a message M is first split into blocks of fixed size $M = M_1, M_2, \ldots, M_n$. Then using the block cipher we compute the sequence $H_0 = a$, $H_i = H_{i-1} \oplus E_{M_i}(H_{i-1})$, where a is a constant. The last value H_k is the tag. Suppose the cipher satisfies the complementary property: If $C = E_K(P)$ then $\neg C = E_{\neg K}(\neg P)$, where $\neg$ denotes bitwise negation. (DES satisfies this property.) Use this property to alternate a message consisting of blocks $M_1, M_2, \ldots, M_k$ so that the tag does not change.

   Show that this approach still works against the scheme based on the rule: $H_i = M_i \oplus E_{H_{i-1}}(M_i)$.

5. Alice wants to send a single bit of information (a yes or no) to Bob by means of a word of length 2. Alice and Bob have 4 possible keys available to perform message authentication. The following matrix shows the 2-bit word sent for each message under each key:

	Message	
Key	0	1
1	00	01
2	10	00
3	01	11
4	11	10

   (a) What is the probability that someone else can successfully impersonate Alice?
   (b) What is the probability that someone can replace an intercepted message with another message successfully?

6. Solve the following exercises in number theory

   (a) Find an integer x such that $37x \equiv 1 \pmod{101}$.
   (b) What is the order of 5 modulo 37?
   (c) Let $n = \varphi(7!)$. Compute the prime factorization of n.
   (d) Prove that 3 is a quadratic residue modulo p (p prime) if $p \equiv 1, 11 \pmod{12}$ and p is a non-residue if $p \equiv 5, 7 \pmod{12}$.
   (e) Let p be a prime and q a primitive root modulo p. Show that a is a quadratic residue modulo p if and only if $a \equiv q^{2k} \pmod{p}$ for some k.