Definition: $\underline{\mathsf{Enc\text{-}Forge}_{\mathcal{A},\Pi}(n)}$: Run $\mathsf{Gen}(1^n)$ to obtain k. Adversary $\mathcal{A}$ is given input 1^n and access to an encryption oracle $\mathsf{Enc}_k(\cdot)$. They output ciphertext c. Let $m := \mathsf{Dec}_k(c)$, and let Q denote the set of all queries that $\mathcal{A}$ asked its encryption oracle. The output of the experiment is 1 iff $m \neq \perp$ and $m \notin Q$.

Definition: Unforgeable: A private-key encryption scheme Π such that for all PPT adversaries $\mathcal{A}$, $\Pr[\mathsf{Enc\text{-}Forge}_{\mathcal{A},\Pi}(n) = 1] \leq \mathtt{negl}(n)$.

Definition: Authenticated: A private-key encryption scheme that is CCA-secure and unforgeable.

Construction: Encrypt-and-authenticate: Given plaintext m, sender transmits $\langle c, t\rangle$, where $c \leftarrow \mathsf{Enc}_{k_E}(m)$ and $t \leftarrow \mathsf{Mac}_{k_M}(m)$. The receiver behaves as expected, obtaining m from $\mathsf{Dec}_{k_E}(c)$, and running $\mathsf{Vrfy}_{k_M}(m, t)$. It is likely the case here that t leaks information about the message (often, MACs are deterministic, breaking CPA-security), and so this is not an authenticated encryption scheme.

Construction: Authenticate-then-encrypt: Given plaintext m, sender transmits c, where $t \leftarrow \mathsf{Mac}_{k_M}(m)$ and $c \leftarrow \mathsf{Enc}_{k_E}(m||t)$. The receiver behaves as expected, decrypting $m||t$ from c, then checking $\mathsf{Vrfy}_{k_M}(m, t)$. If, for example, a CBC-mode-with-padding scheme is used, the decrypt algorithm will return a "bad padding" error, while if the padding passes, Vrfy will return an "authentication failure". This difference can leak information and allow for various attacks on the scheme, so this is not an authenticated encryption scheme.

Construction: Encrypt-then-authenticate: Given plaintext m, sender transmits $\langle c, t\rangle$, where $c \leftarrow \mathsf{Enc}_{k_E}(m)$ and $t \leftarrow \mathsf{Mac}_{k_M}(m)$. The receiver behaves as expected, checking $\mathsf{Vrfy}_{k_M}(c, t)$, then decrypting m as $\mathsf{Dec}_{k_E}(c)$. Of the three listed, this is the only one that is an authenticated encryption scheme (Assuming that Enc is CPA-secure, Mac is strongly secure, and k_E and k_M are chosen independently uniformly at random.)

There are 3 major types of network attacker attacks.

In a reordering attack, an attacker swaps the order of messages sent across a network, making c_2 arrive before c_1.

In a replay attack, an attacker resends messages later.

In a reflection attack, an attacker sends messages from a sender back to them at a later time, which the other person never sent.

The first two attacks can be prevented when A and B (the two people communicating across the network) keep counters, $\mathtt{ctr}_{A,B}$ and $\mathtt{ctr}_{B,A}$, of how many messages have been sent/received in each direction.

A reflection attack can either be prevented by having a reflection bit b to say who the sender is, or by having a different key-set for messages going different directions.

In the $\mathsf{Mac\text{-}forge}^{\text{1-time}}_{\mathcal{A},\Pi}$ experiment, adversary $\mathcal{A}$ outputs m', is given a tag $t' \leftarrow \mathsf{Mac}_k(m')$, then can calculate and think, then output (m, t), $m \neq m'$, which are verified as usual to determine success.

Definition: ε-secure (also one-time ε-secure): A MAC $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ such that for all (even unbounded) adversaries $\mathcal{A}$, $\Pr[\mathsf{Mac\text{-}forge}^{\text{1-time}}_{\mathcal{A},\Pi} = 1] \leq \varepsilon$.

Definition: Strongly universal: A function $h : \mathcal{K} \times \mathcal{K} \to \mathcal{T}$ such that for all distinct $m, m' \in \mathcal{M}$, and all $t, t' \in \mathcal{T}$, it holds that $\Pr[h_k(m) = t \wedge h_k(m1) = t'] = \frac{1}{|\mathcal{T}|^2}$, where the probability is taken over uniform choice of $k \in \mathcal{K}$.

Construction: : Let $h : \mathcal{K} \times \mathcal{M} \to \mathcal{T}$ be a strongly universal function. Define a MAC as follows: Gen: uniform $k \in \mathcal{K}$. Mac: given k, m, output tag $t := h_k(m)$. Vrfy: On input k, m, t, output 1 iff $t \stackrel{?}{=} h_k(m)$.

Theorem: : If h is a strongly universal function, then the above construction is a $\frac{1}{|\mathcal{T}|}$-secure MAC for messages in $\mathcal{M}$.

Theorem: : for any prime p, the function h defined as $h_{a,b}(m) = [a \cdot m + b \mod p]$, where $\mathcal{M} = \mathbb{Z}_p$, and $\mathcal{K} = \mathbb{Z}_p \times \mathbb{Z}_p$, so $(a, b) \in \mathcal{K}$, $m \in \mathcal{M}$, is strongly universal.

Definition: Hash function: A function with output length ℓ is a pair of PPT algorithms (Gen, H) such that $\mathsf{Gen}(1^n)$ outputs a key s, and H takes s and a string $x \in \{0, 1\}^*$, and outputs a string $H^s(x) \in \{0, 1\}^n$, assuming n is implicit in s.

Definition: Compression function (fixed-length hash function for inputs of length ℓ'): a hash function where H^s is only defined for inputs $x \in \{0, 1\}^{\ell'(n)}$, and $\ell'(n) > \ell(n)$.

Definition: $\underline{\mathsf{Hash\text{-}Coll}_{\mathcal{A},\Pi}(n)}$: $s \leftarrow \mathsf{Gen}(1^n)$. Adversary $\mathcal{A}$is given s and outputs x, x'. (If Π is fixed-length, then $x, x' \in \{0, 1\}^{\ell'(n)}$.) The output is 1 (success) iff $x \neq x'$ but $H^s(x) = H^s(x')$.

Definition: Collision resistant: A has function $\Pi = (\mathsf{Gen}, H)$ such that for all PPT adversaries $\mathcal{A}$, $\Pr[\mathsf{Hash\text{-}Coll}_{\mathcal{A},\Pi}(n) = 1] \leq \mathtt{negl}(n)$.

Definition: Second-preimage resistance (target-collision resistance): A hash function such that given s and x, an adversary cannot find x' such that $x' \neq x$ and $H^s(x) \neq H^s(x')$.

Definition: Preimage resistance: A hash function such that given s and y, an adversary cannot find x such that $H^s(x) = y$.

Construction: Merkle-Damgård: Let (Gen, h) be a fixed-length hash function for inputs of length $2n$ and with output length n. Construct (Gen, H) as follows: $\mathsf{Gen} = \mathsf{Gen}$, H: given s and $x \in \{0, 1\}^*$ of length $L < 2^n$, let $B = \lceil \frac{L}{n} \rceil$, pad x so its length is a multiple of n. Consider the padded result as n-bit blocks $x_1, \ldots, x_B$. Set $x_{B+1} = L$. Set $z_0 = 0^n$, as the IV. For $i = 1, \ldots, B + 1$, let $z_i = h^s(z_{i-1}||x_i)$. Output z_{B+1}.

Theorem: If (Gen, h) is collision resistant, then so is (Gen, H).

Construction: Hash-and-MAC: Let $\Pi = (\mathsf{Mac}, \mathsf{Vrfy})$ be a MAC for length $\ell(n)$, let $\Pi_H(\mathsf{Gen}_H, H)$ be a hash function, with output length $\ell(n)$. Construct MAC $\Pi' = (\mathsf{Gen}', \mathsf{Mac}', \mathsf{Vrfy}')$ as follows: Gen': Takes 1^n, choses uniform $k \in \{0,1\}^n$, $s \leftarrow \mathsf{Gen}_H(1^n)$, outputs key $k' = \langle k, s\rangle$. Mac': Given $\langle k, s\rangle$, $m \in \{0,1\}^*$, output $t \leftarrow \mathsf{Mac}_k(H^s(m))$. Vrfy': Given $\langle k, s\rangle$, $m \in \{0,1\}^*$, tag t, output 1 iff $\mathsf{Vrfy}_k(H^s(m), t) = 1$.

Theorem: : If Π is a secure MAC and Π_H is collision resistant, the above construction is a secure MAC for arbitrary-length messages.

Construction: HMAC: Let (Gen_H, H) be a Merkle-Damgård-generated hash function on (Gen_H, h) taking inputs of length $n + n'$. Let $\texttt{opad}$and $\texttt{ipad}$be fixed constants of length n'. Define a MAC as follows: Gen: Given 1^n, $s \leftarrow \mathsf{Gen}_H(1^n)$, uniform random $k \in \{0,1\}^{n'}$. Output key $\langle s, k\rangle$. Mac: Given $\langle s, k\rangle$ and $m \in \{0,1\}^*$, output $t := H^s((k \oplus \texttt{opad})||H^s((k \oplus \texttt{ipad})||m))$. Vrfy: Given $\langle s, k\rangle$, $m \in \{0,1\}^*$, tag t, output 1 iff t recomputes correctly.

Definition: Weakly collision resistant: A Hash function (Gen_H, H) defined as a Merkle-Damgård transform, except with $k = IV$ being uniformly chosen from $\{0,1\}^n$, such that every PPT adversary $\mathcal{A}$ has at most negligible success finding a collision (without knowing k.).

Theorem: : Let $k_{out} = h^s(IV||(k \oplus \texttt{opad}))$, $\hat{y}$ be the length-padded y, including anything before it, $\widetilde{\mathsf{Mac}}_k(y) = h^s(k||\hat{y}$, and $G^s(k) = h^s(IV||(k \oplus \texttt{opad}))||h^s(IV||(k \oplus \texttt{ipad})) = k_{out}||k_{in}$. If G^s is a PRG for any s, $\widetilde{\mathsf{Mac}}_k(y)$ is a secure fixed-length mac for messages of length n, and (Gen_H, H) is weakly collision resistant, then HMAC is a secure MAC for arbitrary-length messages.