Strong and Weak collision resistance

What is Strong Collision Resistance?

Strong collision resistance refers to the property where it becomes extremely hard to get two different inputs that will yield an equal hash value for a given cryptographic hash function. In simpler terms; it is very unlikely that two unrelated messages should have the same hash value.

What is Weak Collision Resistance?

Weak collision resistance, which is also called second preimage resistance, is a cryptographic hash function characteristic in which it is computationally hard to find a message that gives exactly a similar hash value as some given input. This implies that finding another message that hashes to the same value as a particular given one is difficult.

Differences Between Strong and Weak Collision Resistance

Property	Strong Collision Resistance	Weak Collision Resistance
Definition	Strong collision resistance in cryptography refers to an attribute of a cryptographic hash function. This is the situation where it is difficult to compute two different inputs that produce the same hash value.	It is a feature of a cryptographic hash function. That means when one input has been given, it is practically impossible to determine another input which leads to the same hash value as the initial one.
Focus	Any two inputs resulting in the same hash value.	Finding a second input that produces the same hash value as a given input.
Application	Digital signatures, message authentication codes.	Digital certificates, password hashing.
Importance	Crucial for ensuring data integrity and security.	Essential for secure cryptographic protocols and applications.
Example Hash Functions	SHA-256, SHA-3	SHA-256, SHA-3, MD5