**Digital Signature Forgery**

**Description 1**

In a cryptographic digital signature or MAC system, digital signature forgery is the ability to create a pair consisting of a message, *m*, and a signature (or MAC), *sign*, that is valid for *m*, where *m* has not been signed in the past by the legitimate signer.[1]

**Definition 2**

digital signature is a digital string which associated a message with some originating entity. A digital signature forgery happens when an adversary creates valid signatures on a message chosen by someone else. [2]

**Definition 3**

What does it mean to successfully forge a signature?

-Existential Forgery: The adversary succeeds in forging the signature of one message, not necessarily of his choice.

-Selective Forgery: The adversary succeeds in forging the signature of some message of his choice.

-Universal Forgery: The adversary, although unable to find the secret key of the The forger, is able to forge the signature of any message.

-Total Break : The adversary can compute the signer’s secret key. [3]

**In Other Words: Bob forges Alice’s signature and send a message to John. John assumes that Alice is sender of the message. Note that message might be an action performed by one of parties or might contain information.**

**Reference**

[1] Vaudenay, Serge. *A classical introduction to cryptography: Applications for communications security*. Springer Science & Business Media, 2006.

[2] <http://www.utdallas.edu/~muratk/courses/crypto07_files/ds.pdf>

[3] <http://cseweb.ucsd.edu/~mihir/papers/gb.pdf>