Society for Multidisciplinary & Advanced Research Techniques (SMART)
Trinity University, Lagos, Nigeria
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Harmarth Global Educational Services
ICT University Foundations USA
IEEE Computer Society Nigeria Chapter

33rd ECOWAS iSTEAMS ETech Multidisciplinary Conference (ECOWAS-ETech)

Digital Signature Standards and Digital Signature Algorithms

Adu Bernard Yeboah
Ghana Institute of Management & Public Administration
GreenHills Accra, Ghana
E-mail: bernard.adu@st.gimpa.edu.gh

ABSTRACT

Digital Signature Standard (DSS) is a Federal Information Processing Standard(FIPS) which defines algorithms that are used to generate digital signatures with the help of Secure Hash Algorithm(SHA) for the authentication of electronic documents. Digital Signatures Algorithm (DSA) is a FIPS (Federal Information Processing Standard) for digital signaturesIt functions on the framework of modular exponentiation and discrete logarithmic problems, which are difficult to compute as a force-brute system. This piece x-rays these two standards and elucidate their attributes.

Keywords: DSA, DSS, Security, Standards, Signatures, Algorithms.

Proceedings Citation Format
Adu Bernard Yeboah (2022): Digital Signature Standards and Digital Signature Algorithms. Proceedings of the 33rd ECOWAS iSTEAMS Emerging Technologies, Scientific, Business, Social Innovations & Cyber Space Ecosystem Multidisciplinary Conference. University of Ghana/Academic City University College, Ghana. 29th Sept – 1st Oct, 2022. Pp 134-136. www.isteams.net/ghanabespoke2022. dx.doi.org/10.22624/AIMS-/ECOWASETECH2022P27

1. INTRODUCTION

DSS only provides us with the digital signature function and not with any encryption or key exchanging strategies.DSS only provides us with the digital signature function and not with any encryption or key exchanging strategies.

2. DIGITAL SIGNATURE STANDARDS

Sender Side :

A hash code is generated out of the message and following inputs are given to the signature function –

1. The hash code.
2. The random number ‘k’ generated for that particular signature.
3. The private key of the sender i.e., PR(a).
4. A global public key(which is a set of parameters for the communicating principles) i.e., PU(g).

These input to the function will provide us with the output signature containing two components – ‘s’ and ‘r’. Therefore, the original message concatenated with the signature is sent to the receiver.

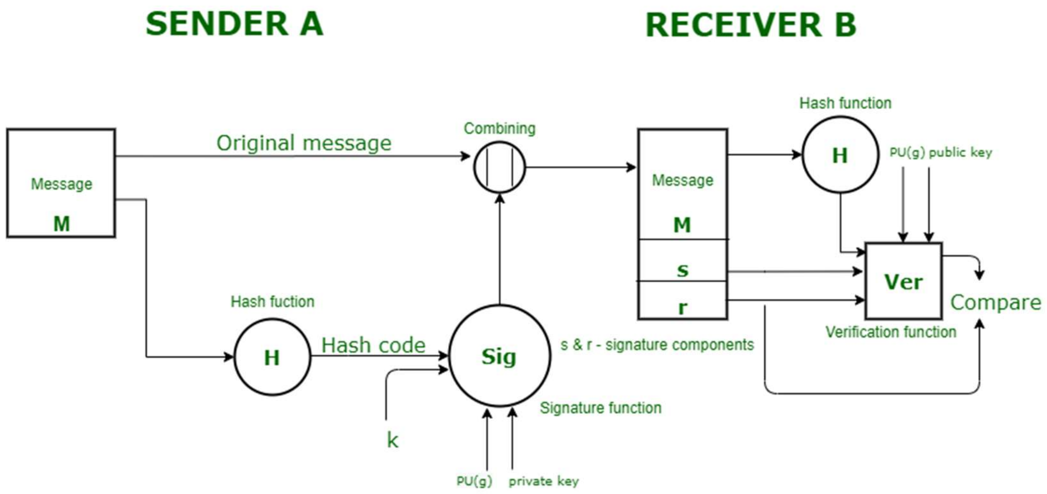

Fig 1: Typical DSS Scenario

Receiver Side :
At the receiver end, verification of the sender is done. The hash code of the sent message is generated. There is a verification function which takes the following inputs –

1. The hash code generated by the receiver.
2. Signature components ‘s’ and ‘r’.
3. Public key of the sender.
4. Global public key.

The output of the verification function is compared with the signature component ‘r’. Both the values will match if the sent signature is valid because only the sender with the help of it private key can generate a valid signature.DSA (Digital Signature Algorithm) incorporates the algebraic properties of discrete logarithm problems and modular exponentiations for generating an electronic signature for various applications.

3. DIGITAL SIGNATURES ALGORITHM (DSA)

Digital Signatures Algorithm (DSA) is a FIPS (Federal Information Processing Standard) for digital signaturesIt functions on the framework of modular exponentiation and discrete logarithmic problems, which are difficult to compute as a force-brute system.
DSA Algorithm provides three benefits, which are as follows:

- Message Authentication: You can verify the origin of the sender using the right key combination.
- Integrity Verification: You cannot tamper with the message since it will prevent the bundle from being decrypted altogether.
- Non-repudiation: The sender cannot claim they never sent the message if verifies the signature..

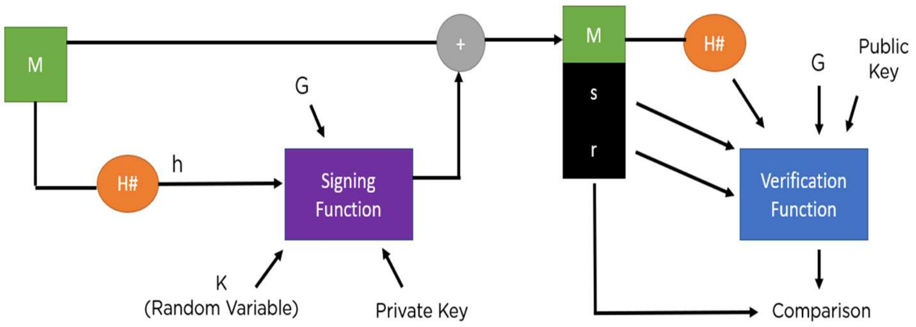

Fig 2: Digital Signature Algorithms

The image above shows the entire procedure of the DSA algorithm. You will use two different functions here, a signing function and a verification function. The difference between the image of a typical digital signature verification process and the one above is the encryption and decryption part. They have distinct parameters.

REFERENCES

Digital Signature Algorithm - Wikipediahttps://en.wikipedia.org › wiki › Digital_Signature_Alg..