

EXPERIMENT 1

Familiarization with CRYPTOOOL

1.1 Aim

To familiarize Cryptool, which is an open source program which enables to apply and analyse cryptographic mechanisms.

1.2 Theory

Cryptool is an open-source program that can be used in various aspects of cryptographic and cryptanalytic concepts. This tool provides graphical interface, better documentation to achieve the encryption and decryption, bundles of analytic tools, and several algorithms. Under Encrypt/Decrypt category, four different groups of algorithms are presented: Symmetric(classic), Symmetric(Modern), Asymmetric and Hybrid. The Classical symmetrical algorithms supported are: Caesar/Rot-13, Vigenere, Hill, Substitution/Atbash, Playfair, ADFGVX, Byte Addition, XOR, Vernam/OTP, Homophone, Permutation/Transposition, Solitaire, Scytale/Rail Fence.

1.3 Familiarise Encryption/Decryption of various methods

1.3.1 Caesar Cipher

A Caesar cipher is a simple method of encoding messages. Caesar ciphers use a substitution method where letters in the alphabet are shifted by some fixed number of spaces to yield an encoding alphabet. A Caesar cipher with a shift of 3 would encode an A as a D, an M as an P, and a Z as a C, and so on. The method is named after Roman leader Julius Caesar, who used it in his private correspondence.

plain: sample text for encryption

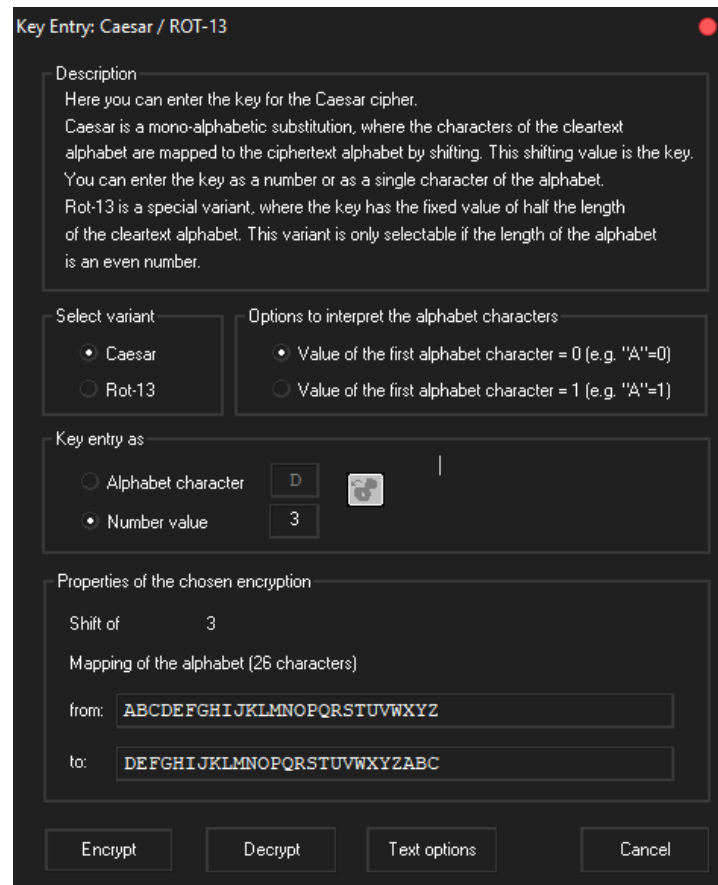
cipher: vdpsoh whaw iru hqfubswlrq

The alphabet is wrapped around, so that the letter following Z is A. The transformation is

defined by listing all possibilities, as follows:

plain: a b c d e f g h i j k l m n o p q r s t u v w x y z

cipher: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C



The dialog box is titled "Key Entry: Caesar / ROT-13". It contains a "Description" section explaining the Caesar cipher and its variant, Rot-13. Below this, there are two sections: "Select variant" with radio buttons for "Caesar" (selected) and "Rot-13", and "Options to interpret the alphabet characters" with radio buttons for "Value of the first alphabet character = 0 (e.g. 'A'=0)" (selected) and "Value of the first alphabet character = 1 (e.g. 'A'=1)". The "Key entry as" section has radio buttons for "Alphabet character" and "Number value" (selected), with input fields showing "D" and "3" respectively. The "Properties of the chosen encryption" section shows "Shift of 3" and a mapping of the alphabet from "ABCDEFGHIJKLMNOPQRSTUVWXYZ" to "DEFGHIJKLMNOPQRSTUVWXYZABC". At the bottom are buttons for "Encrypt", "Decrypt", "Text options", and "Cancel".

Figure 1: Encryption using caesar cipher

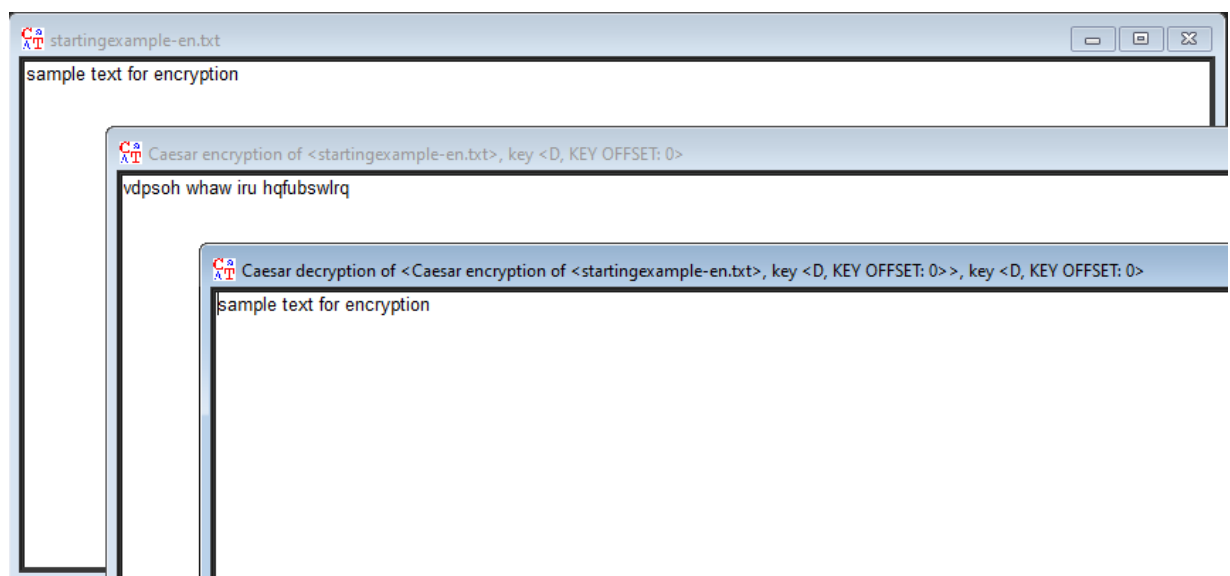


Figure 2: Encrypt/Decrypt text using caesar cipher.

1.3.2 Advanced Encryption Standard

The AES algorithm is a symmetrical block cipher algorithm that takes plain text in blocks of 128 bits and converts them to ciphertext using keys of 128, 192, and 256 bits. Since the AES algorithm is considered secure, it is in the worldwide standard. It is based on a substitution-permutation network, also known as an SP network. It consists of a series of linked operations, including replacing inputs with specific outputs (substitutions) and others involving bit shuffling (permutations).

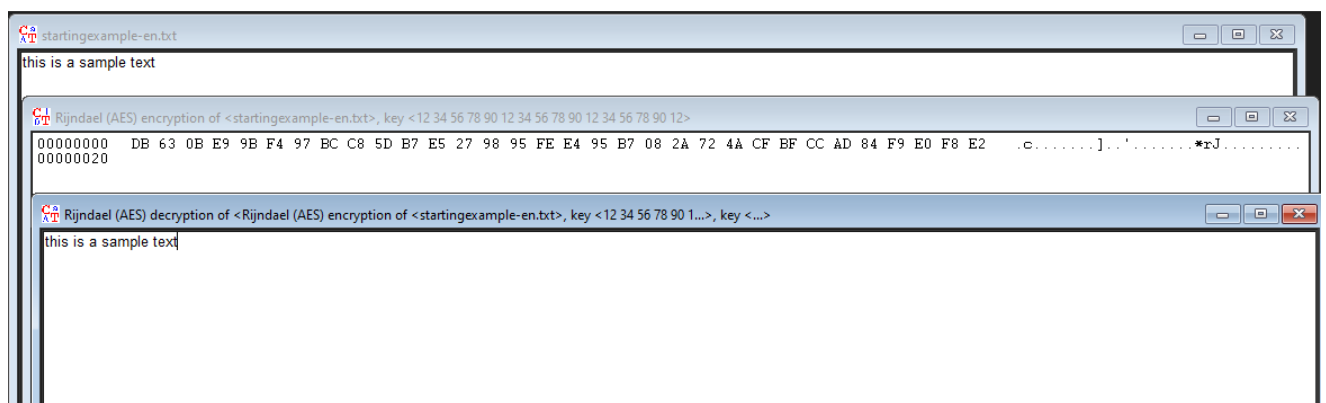


Figure 3: AES encryption/decryption using Cryptool

1.3.3 RSA Algorithm

The RSA algorithm is an asymmetric cryptography algorithm; this means that it uses a public key and a private key (i.e. two different, mathematically linked keys). As their names suggest, a public key is shared publicly, while a private key is secret and must not be shared with anyone.

RSA user creates and publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers are kept secret. Messages can be encrypted by anyone, via the public key, but can only be decoded by someone who knows the prime numbers.

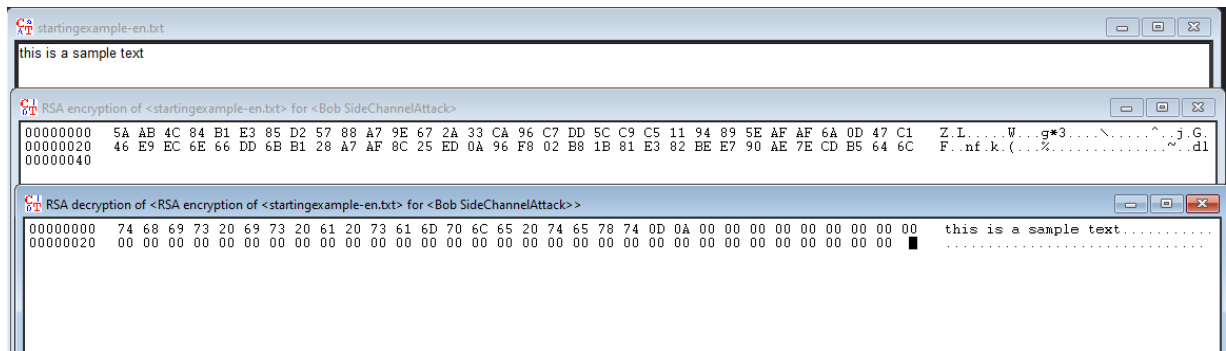


Figure 4: RSA encryption/decryption using Cryptool

1.3.4 Hybrid RSA-AES Algorithm

Hybrid Encryption is a concept in cryptography which combines/merge one/two cryptography algorithms to generate more effective encrypted text. Hybrid Algorithms for the cryptography are effective and so, it is not very easy to detect the pattern and decode the message.

We can combine RSA encryption with AES symmetric encryption to achieve the security of RSA with the performance of AES. This is normally done by generating a temporary, or session, AES key and protecting it with RSA encryption. combine RSA encryption with AES symmetric encryption to achieve the security of RSA with the performance of AES. This is normally done by generating a temporary, or session, AES key and protecting it with RSA encryption.

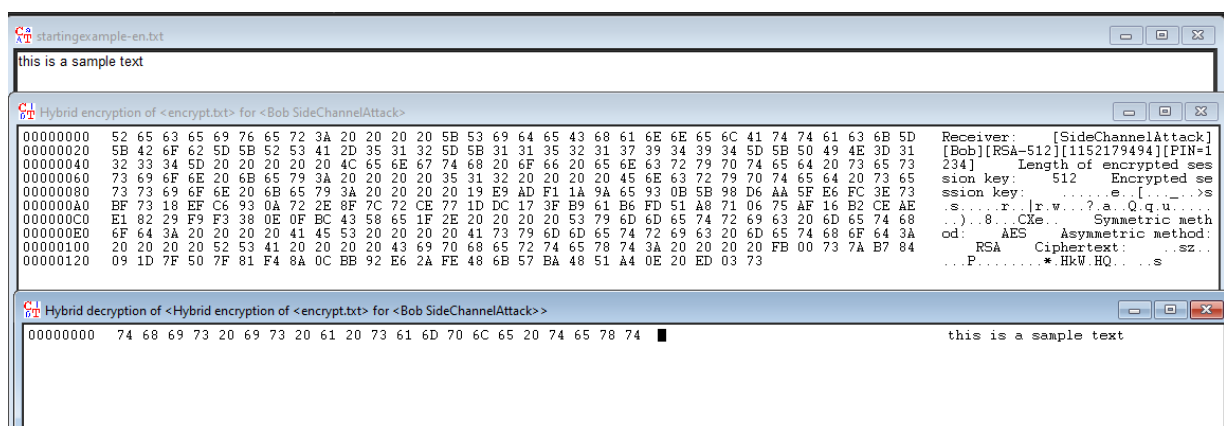


Figure 5: RSA-AES hybrid encryption/decryption using Cryptool

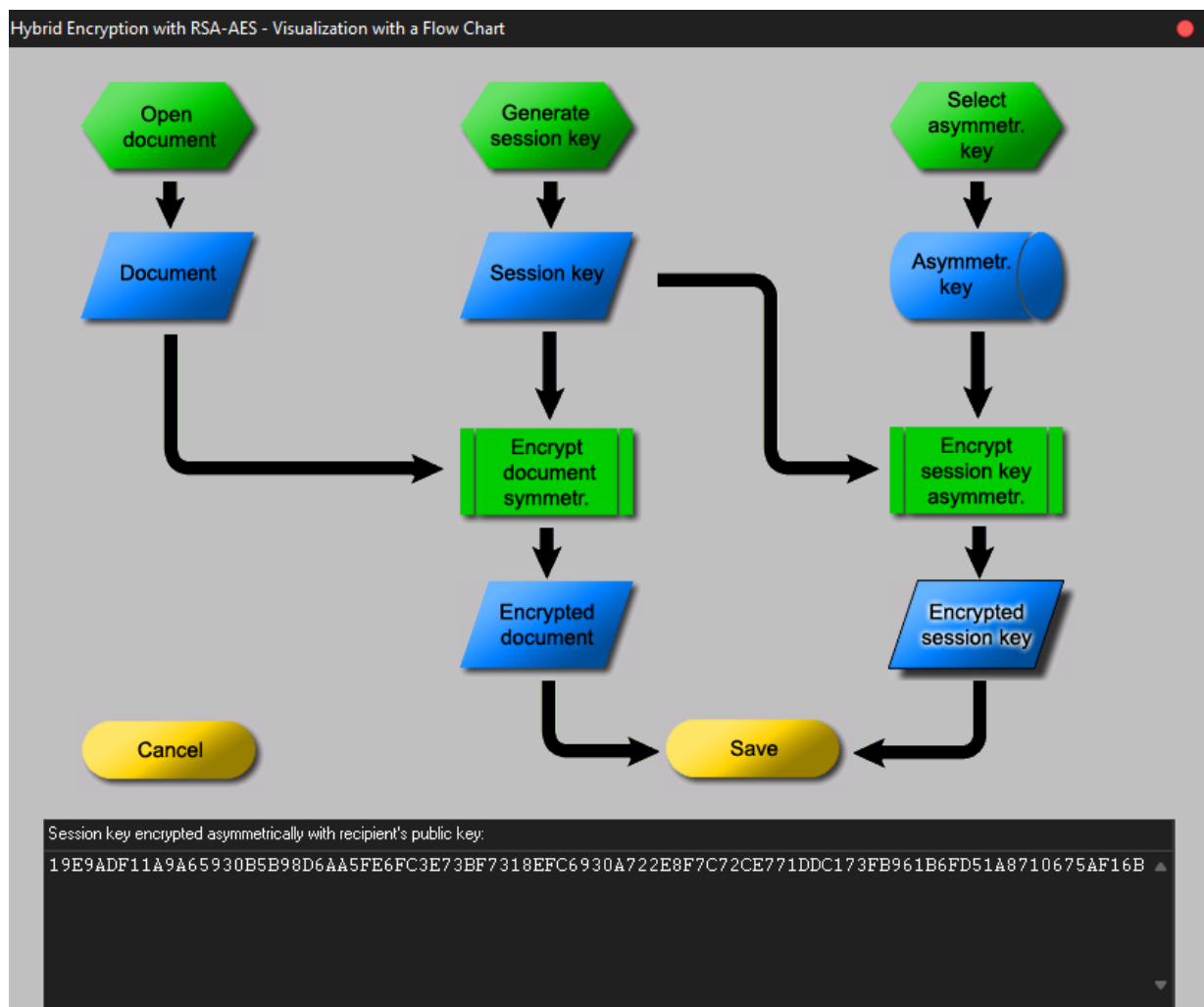


Figure 6: Flow chart of hybrid encryption with RSA-AES

1.4 Cryptanalysis

Cryptanalysis is the art of trying to decrypt the encrypted messages without using the key that was used to encrypt the messages. Cryptanalysis uses mathematical analysis and algorithms to decipher the ciphers. It is used to breach security systems to gain access to encrypted content and messages even the cryptographic key is unknown.

The success of cryptanalysis attacks depends on Amount of time available, Computing power available, Storage capacity available.

The following is a list of the commonly used Cryptanalysis attacks.

1. Brute force attack– this type of attack uses algorithms that try to guess all the possible logical combinations of the plaintext which are then ciphered and compared against the original cipher.
2. Dictionary attack– this type of attack uses a wordlist in order to find a match of either the plaintext or key. It is mostly used when trying to crack encrypted passwords.
3. Rainbow table attack– this type of attack compares the cipher text against pre-computed hashes to find matches

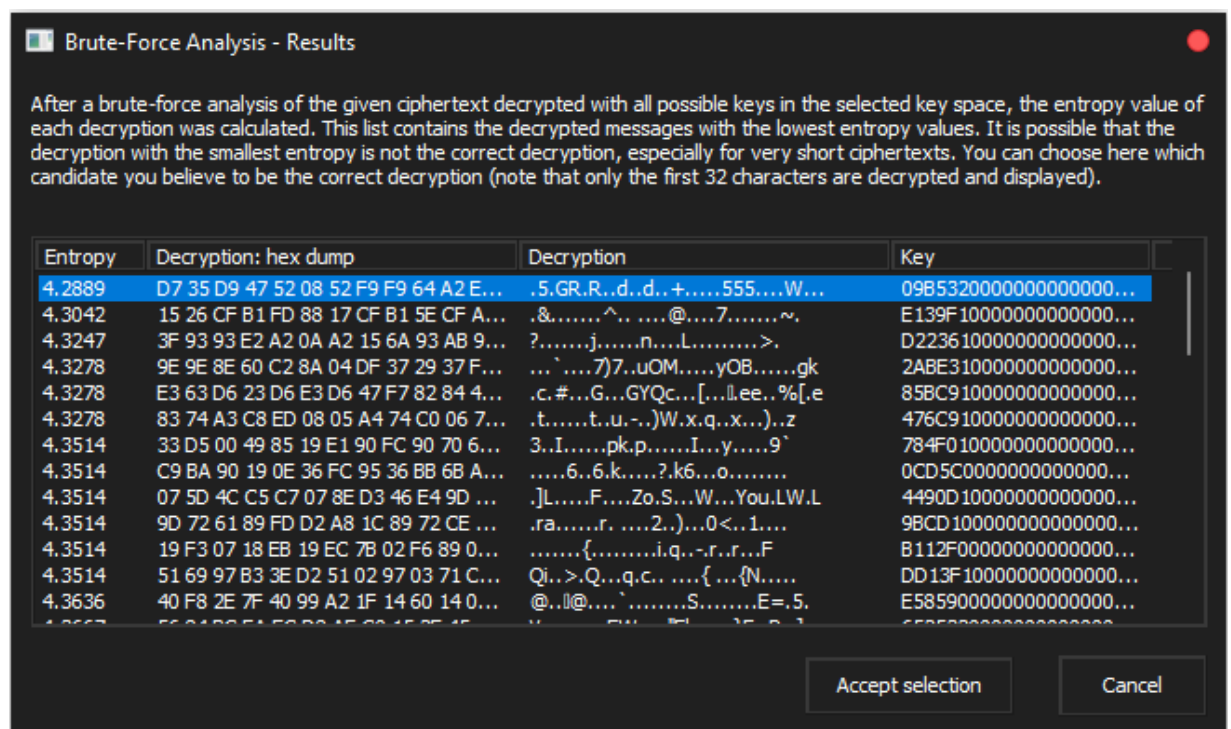


Figure 7: Cryptanalysis of AES Encryption: Key recovery

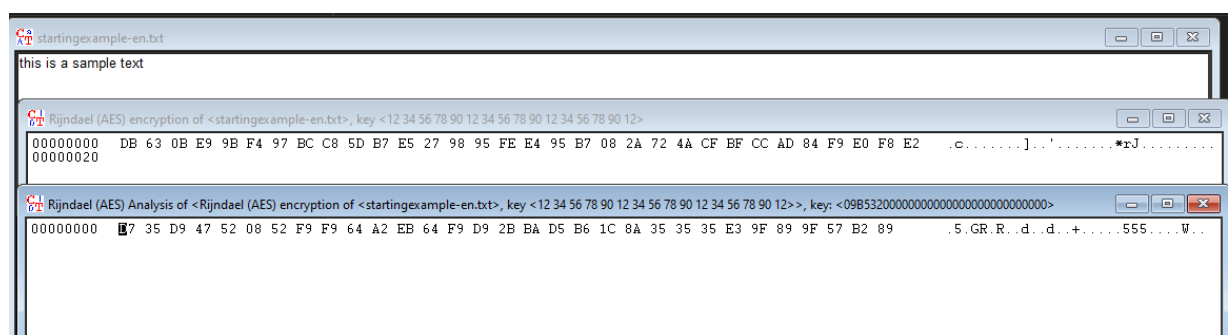


Figure 8: Cryptanalysis of AES Encryption: Key recovery

1.5 Digital Signature generation/ Verification

Cryptographic digital signatures use public key algorithms to provide data integrity. When you sign data with a digital signature, someone else can verify the signature, and can prove that the data originated from you and was not altered after you signed it.

The digital signature is basically a one-way hash of the original data that was encrypted with the signer's private key. To validate the data's integrity, the recipient first uses the signer's public key to decrypt the digital signature. The recipient then uses the same hashing algorithm that generated the original hash to generate a new one-way hash of the same data. Information about the hashing algorithm used is sent with the digital signature. Finally, the recipient compares the two hash values. If they match, the data has not changed since it was signed. If the hashes do not match, the data may have been tampered with since it was first signed or the digital signature may have been created with a private key that does not correspond to the public key presented by the signer.

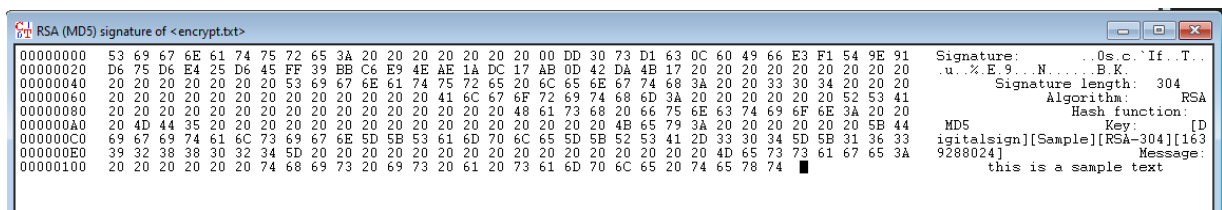


Figure 9: Signature

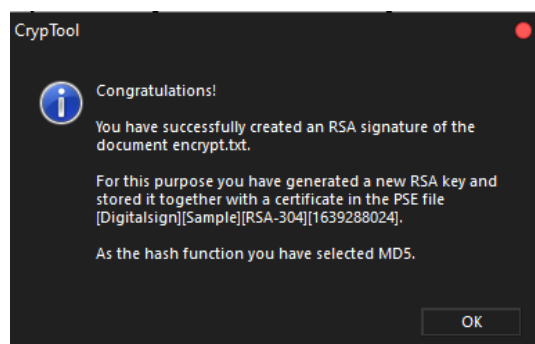


Figure 10: Success response of RSA signature

