Practical Number 8

Aim: To implement Fiat-Shamir protocol for entity authentication using a client server program where the client is the claimant and the server is the verifier.

Theory: Fiat-Shamir is a Zero Knowledge protocol for entity authentication in which the claimant proves to the verifier that she knows a secret, without revealing it i.e. the claimant does not reveal anything that might endanger the confidentiality of the secret. This is unlike the Password based or Challenge-Response based entity authentication protocols where the verifier may misuse the secret of the claimant as he knows it. In zero knowledge entity authentications, the interactions are so designed that they cannot lead to revealing or guessing the secret. After exchanging messages, the verifier only knows that the claimant does or does not have the secret, nothing more. The result is a yes/no situation; a single bit of information.

A trusted third party chooses two large prime numbers p and q to calculate n= p x q. The value of n is announced to the public; the value of p and q are kept secret. The claimant chooses a secret number ***s*** between 1 and n-1 and calculates ***v*** = s^2 mod n. The claimant keeps ***s*** as her private key and registers ***v*** as her public key with the third party. Verification of claimant by the verifier is done in following steps.

1. The claimant chooses a random number ***r*** between 0 and n-1; ***r*** is called the commitment, and calculates ***x***= $\mathbf{r^2}$ **mod n**; ***x*** is called the witness.

2. The claimant sends ***x*** to the verifier as witness.

3. The verifier sends the challenge ***c*** to the claimant. The value of ***c*** is either 0 or 1.

4. The claimant calculates the response as $\mathbf{y = rs^c}$**.**

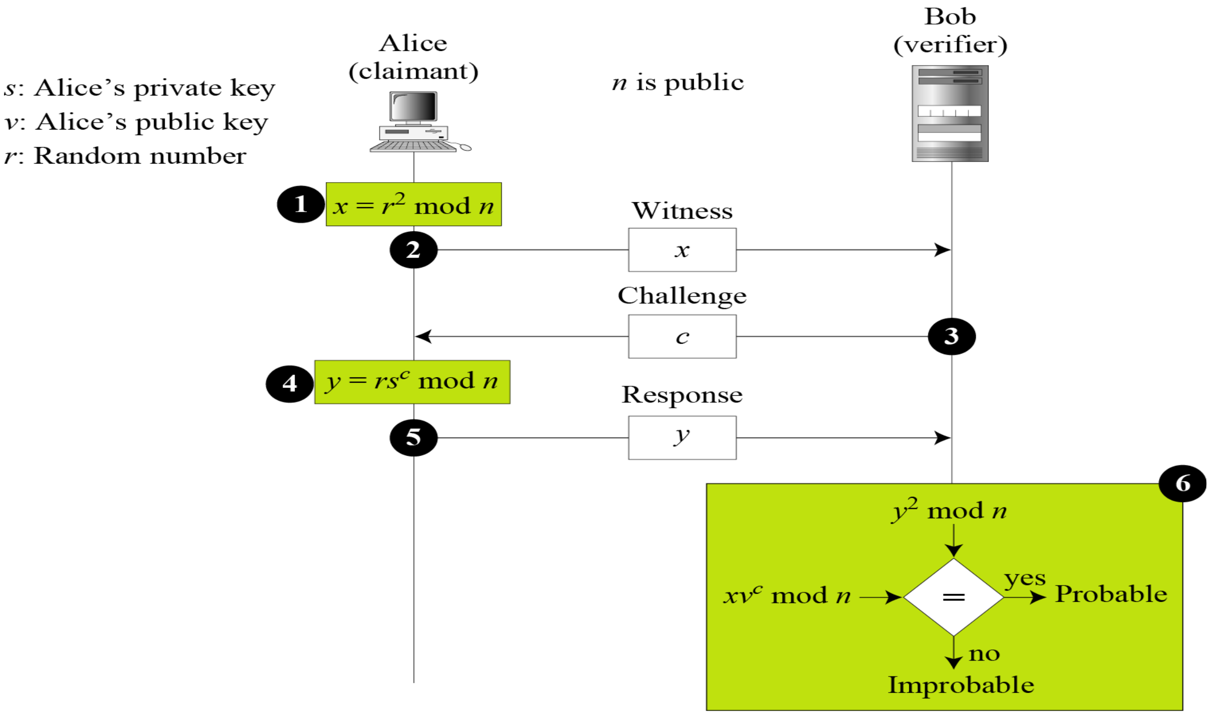
5. The claimant sends the response to the verifier to show that she knows the value of her private key, ***s***. she claims to be the claimant.

6. The verifier calculates y^2 and xv^c. If these two values are congruent, then the claimant
   mod n
   either knows the value of s (honest) or she has calculated the value of y in some other way (dishonest).

$$Y^2 = (rs^c)^2 = r^2 s^{2c} = r^2 (s^2)^c = xv^c$$

mod n

The six steps constitute a round; the verification is repeated several times with the value of c chosen randomly. The claimant passes the test in each round to be verified. If she fails one single round, the process is aborted and she is not authenticated. If The verifier assigns a probability of ½ to each round of the test and the test is repeated 20 times, the probability of a dishonest claimant passing the test reduces to $(½)^{20}$ or 9.54×10^{-7}. It is highly improbable that a dishonest claimant can guess correctly 20 times.



Conclusion: Fiat-Shamir protocol for entity authentication has been studied and successfully implemented.