5616 AS

1 Poker and Cyphers

A.

I used the known plaintext attack. Because the ciphertext and plaintext pair is chosen by Slim and Rusty. I just identify two pairs of their ciphers. I can not select neither the message nor the ciphertext.

C.

I think this PRNG is not secure enough. As this PRNG uses the time as the seed. Everybody knows the time and can use this as the seed to predicate the next random number. So to make this PRNG more secure, I should change the seed to Thermal noise of hard drives, Low-order bit fluctuations of voltage readings, User input or Geiger counter click timing.

E.

If the ciphertext message contains a series of hexadecimal number or just some unreadable strings, the cipher used should be one of the modern symmetric cipher. If the ciphertext message, for example English, only contains the characters in the alphabet of English, the cipher used should be a polyalphabetic substitution cipher.

I will calculate the index of coincidence of this ciphertext message. First, I will divide the ciphertext message into n-size characters set. Second, I will compute the aggregate delta I.C. for all n columns ("delta bar"). Third, I will compare these n Delta-bar I.C. values with the I.C. values of English and Spanish. If the most similar value is English, the plaintext was sent by a Columbian paramilitary group, otherwise, it was sent by a Californian drug dealer.

2 General Questions

B.

Timing attack is one of the side channel attacks. It will take time to execute the cryptographic algorithms. This execution can differ based on the input. Attackers can measure this time and work backwards to the input.

The execution time for the RSA decryption depends on the number of '1' bits in the key. If the system does not hide the finish time of the decryption, attackers can use the public key to encrypt a lot of messages and let the system to decrypt these. Attackers will measure the decryption finish time and work backwards to the RSA private key.

D.

I think the rate of improving attacks on asymmetric cryptosystems is greater than symmetric cryptosystems. Because the security of asymmetric cryptosystems is based on the presumed difficulty of a small set of number-theoretic problems. With the increasing of the computing speed, the problem may be solved very easily. For symmetric cryptosystems, even the basic cipher is not secure, people can use the basic cipher to construct stronger ciphers.

The end game for attacks on asymmetric algorithms is that attackers can use future computing machine to solve the set of number-theoretic problems very quickly, hence the whole algorithms can no be used.

3 Protocols

A.

To convince Bob that some other value ≠ is the committed value, Alice can ask Bob to calculate h(x||r) with x received during the open phase and r received during the commitment phase, denote the result of this calculation as . Bob can check if received during the commitment phase. As MD5 has the Collision Resistance property, if they are the same, x received during the open phase should be the same as the committed value.

B.

Bob can use the collision attack to find x||r with given y during the commitment phase. The best collision attack can only take times attempt, this won’t take too much time with a regular pc. After finding x||r, Bob can use r to determine the committed value.

C.

Commitment phase:

First, Alice generates random strings r, s, and computes y = SHA256(r||s||x). Second, Alice sends Bob r and y.

Revelation Phase:

Alice sends Bob the remaining data of s and x. Then Bob verifies that SHA256(r||s||x) is the same as the y he received.

With this scheme, even Bob brute force the value of r||s||x, Bob can not determine the value of x, because s is kept secret.

4 Network and Software Security

A. SSL

Whether a website has a 256-bit certificate is not the standard to prove that the website is secure. When getting the website’s certificate, it should be checked if one of the trusted Certification Authority has signed the certificate. Sometimes the verification can be cancelled with Online Certificate Status Protocol by the attackers and this make the users do not know the website is not secure. Sometimes there can even be some fraudulent certificates.

B.

The difference between the salt and the secret salt is that salt can be either public or secret. Actually, the salt is not necessary to be kept secret. An attacker won't know in advance what the salt will be, so they can't pre-compute a lookup table or rainbow table. It is important that the salt can not be reused. Using a single salt also means that every user who inputs the same password will have the same hash. This makes it easier to attack multiple users by cracking only one hash.