2021 spring, Internet Security, final, 2 - 3pm

1. Assume a hash function h(•) follows a Random Oracle. If the number of possible hash values is n, then the probability of no collisions after k distinct hash inputs is given by

How many distinct inputs should be tried for h(•) if the collision probability is 0.5? Write the intermediate equations as well. You can use the following. (20p)

If x is small, 1-x is approximated by e-x. Also approximate sqrt(2 ln 2) by 1.

2. When we compare a blockchain (as a data structure) and a Merkel tree, explain why each of the following sentences is correct or wrong. (20p)

(1) appending an element to a blockchain has more computational complexity than to a Merkel tree

wrong, 블록체인은 linked list 구조고 merkel tree는 binary 트리 구조기 때문에 새로운 object 를 삽입하는데 걸리는 시간은 o(1)과 O(logn) 이다.

(2) updating an element of a blockchain has more computational complexity than of a Merkle tree.

Update 는 search와 big O notation이 같다. Linked list 의 search time 은 o(n) 이고 binary tree 는 O(log N) 이니까 true

3. In DSA signature, r=(gk mod p) mod q and s=[k-1(H(M)+xr)] mod q. Also, y = gx mod p; w = s-1 mod q; u1 = [H(M)w] mod q; u2 = (rw) mod q; and v = [(gu1 yu2) mod p] mod q. The verifier receives the signature (r, s) and message M. How can he check whether the signature is right? Explain the equations to check the signature. Note that g, p, q are public parameters for the DSA signature where p = qr+1 and g is the generator of a subgroup whose size is q; x and k are the secret key and the random number decided by the signer, respectively. H(•) is a hash function.

V = r

4. What are the root causes that make the Internet suffer from IP prefix hijacking attacks and DNS poisoning attacks? What is your opinion? (20p)

DNS response 와 IP prefix announcement 에 authentication 이나 signature가 없고 모든 response를 다 진실된 response라고 믿기 때문에 발생하는 문제이다.

5. Explain how doubleclick, an ad-network company, can track user visiting sites. (20p)

유저의 브라우저가 bing 이라는 사이트를 방문했을 때, 이 사이트 내부에 있는 ad image는 유저에게 서드파티쿠키를 보내고 유저는 이를 저장한다. 유저가 ebay 등의 ad가 있는 다른 사이트를 방문하면, 이 쿠키가 ad 회사에게 가고, 광고회사는 이를 분석해서 유저가 방문한 사이트의 기록을 알아낼 수 있다.

