Assignment - 2

Hash function attacks :-

What is hashing ?

Hashing is simply put, taking an input string of any length and giving out an output of a fixed length cryptographic hashing refers a special class of hash functions with set properties to be considered secure, a cryptographic hash function needs to include properties such as always getting a cosistent result irrespective of how many times you parse through an input, quick computation, and pre-image resistant amo -ng others.

In case of crypto currencies such as bit coin the transactions are taken as an input and run through a hashing algorithm (Bit coin uses SHA-256] which given an output of a fixed length.

Each input has its own unique hash.

Eg:- take inputs ~~has its own~~ A and B where H(A) and H(B) are their respective hashers. It is infeasible for H(A) to be equal to H(B) Infeasible but unfortunately not impossible.

What is a hash function attack?

A Hash function attack is an attempt to find how input strings of hash function that produce the same hash result. Because hash functions have infinite input length and a predefined output length, there is a inevitably going to be the possibility of two different inputs that produce the same output hash.

A hash collision occurs when two separate Inputs produce the same hash output. This can be Exploited by an application that compares two hashes together (such as password hashes, file integrity checks) However the odds of a collision are Extremely low,

Especially for functions with a large in output size such as lengthy and widespread document formats or protocols but as available computational power increases, the ability to attack hash functions becomes more feasible

Types of hash ~~function~~ attacks ?—

There are several ways a hash collision could be exploited. There are mainly three types of hash function attacks.

Collision attack :—

A collision attack on a cryptographic hash tries to find two inputs producing the same hash value. The attacker does not have control over the content of the message, but they are arbitarily chosen by the algorithm In this case, $H(A)$ is equal to be $H(B)$.

Pre-image attack :-

In contrast to a collision attack, in pre-image attack the hash value is specified

(ii) Birthday attack :-

The birthday attack is based on the birthday paradose i.e; the probability that in a set of 'n' randomly chosen people, some pair of them will have the same birthday Applied to hash function attacks, this means you have a 50% chance to break the collision resistance.

How to secure the hash functions :-

No hash-function is collision free, but it usually takes extremely long to find a collision.

Even if a hash function has never been broken a successful attack against a weakened variant may undermine the experts confidence and lead to its abandonment. In the past, weakness had been found in several then popular hash functions including SHA-0,

RIPEMP and MD5. These weaknesses called into question the security of stronger algorithms ~~delete~~ derived from the weak hash functions such as the SHA-1, RIPEMD-128 and RIPEMD-160

Also, there are applications of cryptographic hash functions that donot rely on collision resistance. This means that collision attacks do not affect their security.

Eg:- HMAC's are not vulnerable for the hash attack to be successful, the attacker must be in control of the input to the hash function.

Are hash function attacks something to worry about :-

The Trust is that it depends on the hash function. Even MD5 and SHA-1 are not comple-tely collision resistant. but stronges functions such as SHA-256 appear to be safe far now.

(1) security aspects of RSA algorithm?

RSA security relies on the computational difficulty of factoring large integer. As computing power increases and more efficient factoring algorithms are discovered, the ability to factor larges and larger numbers also increases.

Encryption strength is directly tied to key size and doubling key length can delives an Exponential increase in strength, although it does impair performance RSA keys are typically 1024 or 2048 bits long, but experts believe that 1024 bit keys are no longer fully secure against all attacks. this is why the government and some industries are moving to a minimum key length of 2048 bits.

Barring an unforeseen break through in quantum computing, it will be many years before longer keys are required, but elliptic curve cryptography (ECC) is gaining favor with many security experts as an alternative to RSA to implement public key cryptography. it can create faster, smaller and more efficient cryptographic keys.

Modern hardware and software are Ecc-ready and it's popularity is likely to grow, as it can delivers equivalent security with lower computing power and battery resource usage, making it more suitable for mobile apps than RSA finally, a team of researchers, which included Adi shamir, a co-inventor of RSA, has successfully created a 4096 bit RSA key using acoustic cryptoanalysis, however, any Encryption algorithm is vulnerable to attack.

② Additive Rules of eliptic curve cryptography?

There is a rule called the chord-and-tangent rule, for adding two points on an eliptic curve E(fp) to give a third eliptic curve point, together with this addition operation, the set points E(fp) forms with O serving as the identity. It is this group that ~~called~~ is used in construction of eliptic curve cryptosystems. The addition rule is best Explained geometrically; let $P=(x_1, y_1)$ and $Q=(x_2, y_2)$ be two distinct point on an eliptic curve E. Then the sum of P and Q denoted by $R=(x_3, y_3)$ is defined as follows.

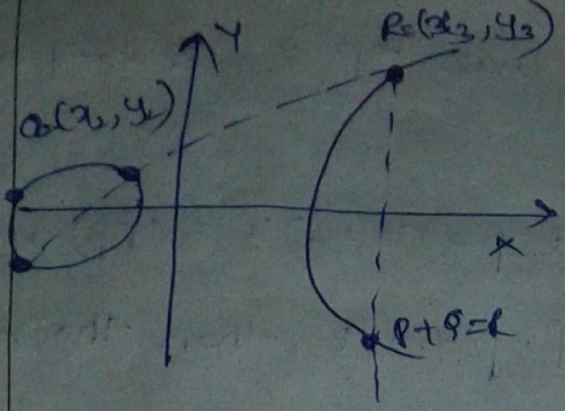

fig4:- geometric description of the addition of two distinct elliptic curve P+Q=R

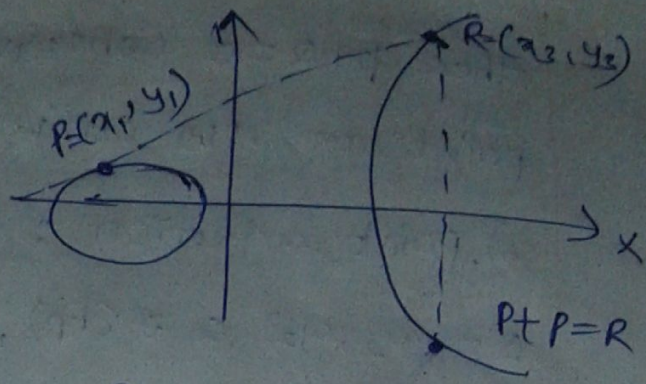

fig5: geometric description of the addition of two distinct elliptic curve P+P=R

Mechanics of EC arithmetic operations :—

All of the arithmetic operations make perfectly good sense modulo p, provided that the denominators are relatively prime to p. Specifically, we define the operation ∂ modulo p (∂ is the identity) by the following arithmetic operation :

Let the points P=(x1, y1) and Q=(x2, y2) be in the elliptic group Ep(a,b) and O be the point at infinity.

The rules for addition over the elliptic group Ep(a,b) are :

1) P+O = O+P for all P ∈ E(fp)

2) If P=(x,y) ∈ E(fp) and if x2=x1 and y2=y1, that is P=(x1, x2) and Q=(x1, x2), (x1, -y1)=-P

then $P+Q=O$ (observe that $-P$ is indeed a point on the curve)

3) point addition : Let $P=(x_1,y_1) \in E(F_p)$ and $Q=(x_2,y_2) \in E(F_p)$, if $P \neq \pm Q$, then their sum $P+Q=(x_3+y_3)$

4) point doubling : Let $P=(x_1,y_1) \in E(F_p)$ and, if $P \neq -P$ then $2P=(x_3+y_3)$

define x_3 and y_3 by

$$x_3=(\lambda^2-x_1+x_2) \bmod p$$

and

$$y_3=\lambda(x_1-x_2)-y \bmod p$$

where

$$\lambda=\begin{cases} y_2-y_1/x_2-x_1, & \text{if } P \neq Q, \text{ point addition} \\ 3x_1^2-a/2y, & \text{if } P=Q, \text{ point doubling.} \end{cases}$$