Kriptolamayı tanımlayarak mutlak ve hesaplamaya bağlı güvenlik ile Kriptografik algoritmalarında ayrık logaritma problemi nedir? Kısaca açıklayınız?

* CRYPTOGRAPHY 🡪 STUDY OF ENCRYPTION PRINCIPLES/METHODS
* CRYPTANALYSIS: Key’i bilmeden şifreyi çözmek (istatistiksel yöntemlerle. Objective to recover key not just message.) 🡪 OBJECTIVE TO RECOVER KEY, NOT JUST MESSAGE
* CRYPTOLOGY = CRYPTOGRAPHY + CRYPTANALYSIS
* …
* Unconditional security: kırılamayan şifre. Encryption fonksiyonu birebir değil.
* Computational security: given limited computing resources, the cipher cannot be broken
* …
* inverse problem to exponentiation is to find the discrete log of a number modulo p
* The discrete logarithm problem is a mathematical problem that forms the basis for several cryptographic algorithms, particularly those used in public key cryptography. In simple terms, the discrete logarithm problem involves finding the exponent x in the equation g ≡ ℎx (mod p) where g, ℎ, and p are known values. Here, g is the base, ℎ is the result of exponentiation, and p is a prime number. 🡪 x = loghg(mod p)
* The problem is considered computationally difficult, especially when p is large, making it infeasible for an attacker to efficiently compute the discrete logarithm without knowledge of the private key.

cryptoghraphic function: plaintext -> ciphertext

[a mod n – b mod n] mod n = (a - b) mod n

* a = hn + a mod n
* b = kn + b mod n
* (a-b) mod n = (a – b – (h+k)n) mod n = [(hn + a mod n) – (kn + b mod n) – hn – kn] mod n

= (a mod n – b mod n) mod n

(ab) mod n = (a mod n) (b mod n )

* (ab) mod n = r
  + ab = kn + r
* a mod n = r1
  + a = k1.n + r1
* b mod n = r2



* + b = k2.n + r2
* ab = (k1.n + r1)(k2.n + r2)



* + ab = n2.k1.k2 + n.k1.r2 + n.k2.r1 + r1.r2
  + ab = n(n.k1.k2 + k1.r2 + k2.r1) + r1.r2



k4

* + ab = n.k4 + r1.r2
  + (ab) mod n = r1.r2
  + (ab) mod n = r
* r = r1.r2

Yerine koyma ve yer değiştirme tabanlı şifreleme nedir? Sakıncaları nelerdir ve çözümleri nelerdir açıklayınız?

* substitution: plaintext’in harfleri başka harf sayı veya sembollerle değiştirilir.
* transposition: hide the message by rearranging the letter order
* …
* Bu tür şifreleme teknikleri genellikle basit ve hızlıdır, ancak modern kriptografik standartlara göre güvenlik düzeyleri düşüktür.
* Sakıncaları:
  + Kolay Kırılabilirlik: Yerine koyma ve yer değiştirme tabanlı şifreleme teknikleri genellikle frekans analizi gibi basit yöntemlerle kolayca kırılabilir. Mesela, dildeki harf frekanslarına dayanarak şifreli metni analiz ederek orijinal metni bulmak mümkündür.
  + Anahtar Uzayının Küçüklüğü: Bu tür şifreleme teknikleri genellikle sınırlı anahtar uzayına sahiptir, yani şifreleme için kullanılabilecek anahtar sayısı sınırlıdır. Bu durum, kaba kuvvet saldırılarına karşı direnci azaltır.
  + Kolay Öngörülebilirlik: Şifreleme sırasında kullanılan basit matematiksel veya mantıksal işlemler, şifreleme sürecini kolayca anlayabilir kılabilir ve bu da şifreyi çözmeyi kolaylaştırabilir.
* Çözümler:
  + Güçlü Anahtar Kullanımı: Anahtar uzayını genişletmek ve kaba kuvvet saldırılarına karşı direnci artırmak için daha uzun ve karmaşık anahtarlar kullanılabilir.
  + Modern Şifreleme Algoritmaları: Klasik yerine koyma ve yer değiştirme tekniklerinin yerine, modern kriptografik algoritmalar kullanılmalıdır. Bu algoritmalar, daha karmaşık matematiksel işlemler ve daha güvenli anahtar uzayları kullanarak daha güçlü şifreleme sağlar.
  + Rastgeleleştirme: Şifreleme sürecinde rastgeleleştirme eklemek, şifrelenmiş verinin daha tahmin edilemez hale gelmesini sağlar.
  + Dijital İmza ve HMAC Kullanımı: Verinin bütünlüğünü sağlamak ve doğrulamak için dijital imza ve HMAC gibi güvenlik katmanları eklemek önemlidir.

vigenere için kasiski (frekans bulup blok boyutunu çıkarır)

kasiski’yi bypass için autokey cipher

Güçlü şifreleme algoritmaları için gerekli yöntemler nelerdir? Şifrelemeyöntemlerini açıklayınız ve brute force saldırılarına zorlanmalarının sebeplerini belirtiniz?

* Anahtar Uzayının Genişliği: Güçlü bir şifreleme algoritması, kullanılan anahtar uzayının geniş olmasını sağlar. Bu, kaba kuvvet saldırılarına karşı dayanıklılığı artırır, çünkü saldırganların doğru anahtarı tahmin etmeleri daha zor hale gelir.
* Karmaşıklık ve Matematiksel Güçlük: Güçlü şifreleme algoritmaları, matematiksel olarak karmaşık işlemleri içerir. Örneğin, RSA algoritması gibi algoritmalar, büyük asal sayıları çarpmak gibi karmaşık matematiksel işlemler kullanarak güvenlik sağlar.
* Rastgeleleştirme: Şifreleme işlemleri sırasında rastgele elemanlar eklemek, şifrelenmiş metni tahmin edilemez hale getirir. Bu, saldırganların şifreleme algoritmasını analiz ederken veya kaba kuvvet saldırıları yaparken daha fazla zorluk yaşamalarını sağlar.
* Döngüsel İşlemler: Güçlü şifreleme algoritmaları, birçok döngüsel işlem içerir. Bu, aynı anahtarın farklı girişlerle kullanılması durumunda dahi farklı çıktılar elde edilmesini sağlar.
* Avalanche Etkisi: Avalanche etkisi, şifreleme işlemi sırasında küçük bir giriş değişikliğinin çıktıda büyük bir değişikliğe yol açmasıdır. Bu özellik, girişin her bir bitinin çıktıya etkisinin eşit ve tahmin edilemez olmasını sağlar.
* ….
* Küçük Anahtar Uzayı: Eğer kullanılan anahtar uzayı küçükse, saldırganlar kaba kuvvet saldırılarıyla hızla tüm olası anahtarları deneyebilirler.
* Zayıf Anahtarlar: Eğer kullanılan anahtarlar belirli bir desene veya zayıf bir algoritma tarafından üretiliyorsa, saldırganlar brute force saldırılarını daha etkili bir şekilde gerçekleştirebilirler.
* Zayıf Şifreleme Algoritması: Eğer kullanılan şifreleme algoritması zayıfsa veya kriptoanaliz yöntemleriyle kırılmışsa, brute force saldırıları daha etkili olabilir.

diffusion: dissipates statistical structure of plaintext over bulk of ciphertext

confusion: makes relationship between ciphertext and key as complex as possibe

Confusion:

* Principle that aims to make the relationship between the encryption key and the ciphertext as complex and intricate as possible.

Avalanche effect with confusion: This implies that not only does a small change in the plaintext cause a significant change in the ciphertext (avalanche effect), but the relationship between the encryption key and the resulting ciphertext is also intricate and difficult to decipher (confusion).

MAC (Message Authentication Code):

* Açıklama: Bir mesajın bütünlüğünü ve kimliğini doğrulamak için kullanılan bir kod veya değerdir.
* İşlevi: Veri bütünlüğünü ve kimliğini korumak için kullanılır. Gönderen tarafından bir anahtar ve bir mesaj kullanılarak oluşturulur, alıcı tarafında bu MAC değeri kullanılarak mesajın bütünlüğü ve kimliği doğrulanır.
* Kullanım Alanları: Veri iletimi sırasında veri bütünlüğünü sağlamak ve kimlik doğrulaması yapmak için kullanılır.

Hash Fonksiyonu:

* Açıklama: Belirli bir giriş verisini alır ve sabit bir uzunluktaki bir çıktı üretir. Bu çıktı genellikle "hash" olarak adlandırılır.
* İşlevi: Özellikle veri bütünlüğü kontrolü, veri arama ve veri depolama gibi birçok uygulama için kullanılır. Aynı giriş her zaman aynı çıktıyı üretir (deterministik).
* Kullanım Alanları: Parola depolama, dijital imzalar, veri bütünlüğü kontrolü gibi birçok güvenlik ve bilgi işlem uygulamasında kullanılır.

Unlike a regular hash function that produces a fixed-size output, a MAC involves a secret key. The key is used along with the message as input to generate a unique code, known as the MAC tag. The MAC tag is sent along with the message.

Collision resistant:

* A hash function is considered collision-resistant if it is computationally infeasible to find two distinct inputs that produce the same hash value (i.e., a collision). In other words, a collision-resistant hash function ensures that it is difficult for an attacker to find two different inputs that map to the same hash output.

D – H (Diffie - Hellman) yönteminin çalışmasını yazınız?

* DH is algorithm for key exchange. For asymmetric algorithms.
* Depends on 2 large prime numbers: n and g 🡪 anyone can know
* Alice has x private number
* Bob has y private number
* Alice calculate A:
  + A = gx(mod n)
* Bob calculate B:
  + B = gy(mod n)
* Alice sends A to Bob, Bob sends B to Alice
* Alice calculates her key K:
  + K = Bx(mod n)
* Bob calculates his key K:
  + K = Ay(mod n)
* Now they have same key

Euler’s Totient

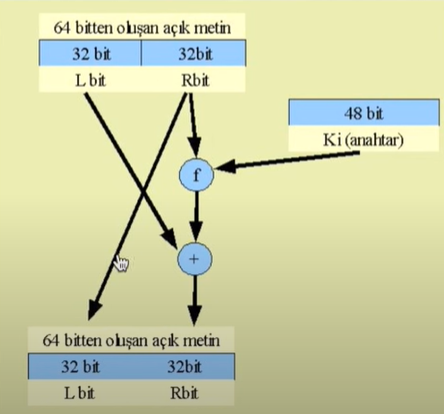
* F(n) 🡪 # of positive integers less than n that are relatively prime to n
* The Euler's totient function plays a key role in the generation of the public and private keys in RSA.

One way trapdoor:

* A trapdoor function is a mathematical function that is easy to compute in one direction but difficult to compute in the opposite direction without special information called the "trapdoor." The trapdoor information makes it feasible to efficiently compute the inverse of the function.

DES

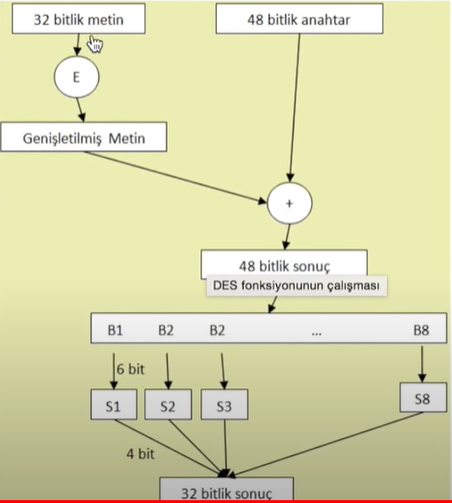
* Mesaj bitlere çevrilir
* Mesajlar 64 bitlik parçalara bölünür – 8 harflik bloklar
* Ayrıca 64 bitlik key var 🡪 her blok için aynı

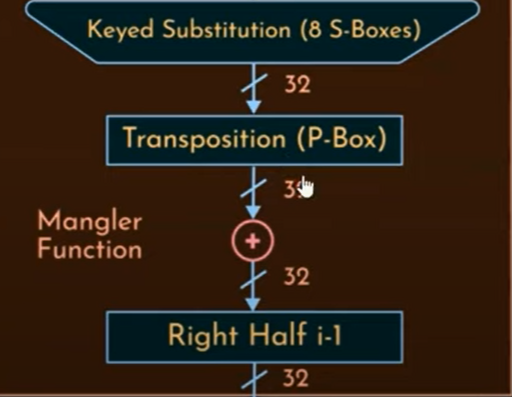


* Bu yapı 16 kez tekrarlanır.
* 64 bitlik anahtar f fonksiyonunda 48 bit çünkü:
  + 8 bit kontrol biti (parity bit)
  + her 16 tekrar için 56 bitten farklı bir 48 bitlik anahtar üretilir S

At the beginning -> initial permutation, at the end 🡪 inverse initial permutation

f fonksiyonu:





* E 🡪 Expansion table
  + A white square with black numbers and a hand pointing at it

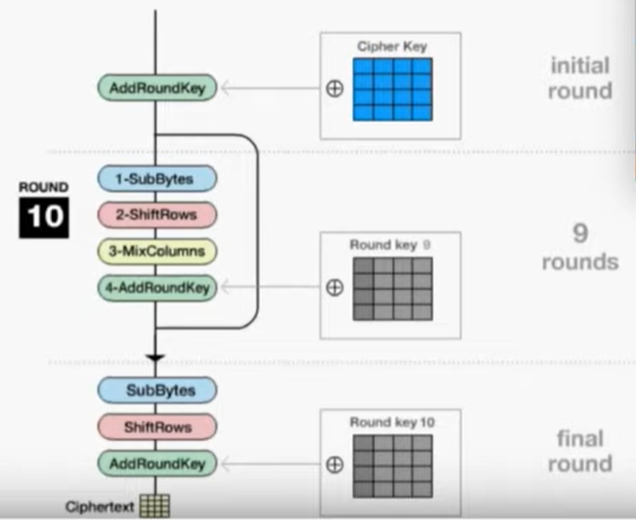
    Description automatically generated
  + 32 bit 🡪 48 bite genişler
* anahtarla xorlanan metni 6 bitlik 8 tane bloğa bölüyoruz.
* 6 bitlik bloklar s-box’lara (substitution box) girer ve 4 bit olarak çıkar
* Anahtar üreteci:
* A screenshot of a computer

  Description automatically generated
* ortadaki 48 bit kullanılır.
* ---
* şifreli mesajı aynen des’e girdi olarak verirsen ve yanına aynı anahtarı verirsen bu sefer çıktı olarak açık mesaj verilir

RSA (Asimetrik)

* 2 tane asal sayı p ve q seçilir (büyük olmalılar)
* n = pq
  + n 🡪 public
  + 2 prime’ın çarpımını geri çarpanlarına ayırmak zor
* (n) = (p-1)(q-1)
  + sadece p’ye bölenler hariç bütün sayılar p ile asal olacak
  + sadece q’ya bölenler bütün sayılar q ile asal olacak
* 1 < e < (n)
  + e 🡪 public key
  + e sayısı ile (n) aralarında asal
* de = 1 mod((n))
  + d 🡪 private key
  + d sayısı extended Euclid ile bulunur
* c = memodn
* m = cdmodn

AES

* Symmetric
* block uzunluğu: 128 bit
* key lengths supports: 128, 192, and 256 bits
* 
* her roundda key oluşturuyoruz.
* SubBytes (Substitute bytes)
  + A diagram of a graph

    Description automatically generated
  + soldaki kutu original mesaj. Her küp 2 hexadecimal, yani 8 bit. Tüm kutu 128 bit (block sayısı).
  + 8 bitlik kutuyu 4 bit + 4 bit olarak düşün
  + 4 bit 16 değer gösterebilir.
  + 16x16 tabloda ilk 4 bit satır, ikinci 4 bit kolon belirtir. O yerdeki 8 biti koyarsın.
  + 16x16 tabloda her kutu 8 bit.
* ShiftRows (transposition)
  + A white and black squares with numbers

    Description automatically generated with medium confidence
  + 2. satır 🡪 1 sola
  + 3. satır 🡪 2 sola
  + 4. satır 🡪 3 sola
* MixColumns
  + A diagram of a block diagram

    Description automatically generated
  + Çarpım matrisiyle her kolonu çarpıyorsun.
* Add Round Key
  + A diagram of a sub key

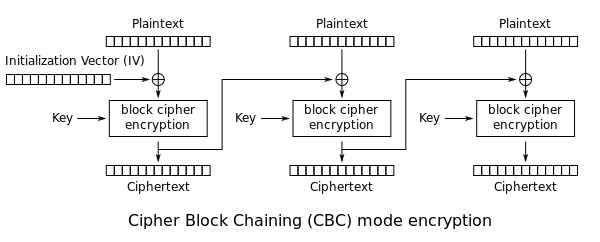
    Description automatically generated with medium confidence
  + 32 bitlik 4 parçadan oluşan key
  + Çıkan sonuç bu round’un sonucu
* Anahtar üretme:
* A screenshot of a computer

  Description automatically generated
* Mavi alan 🡪 128 bitlik ilk orijinal anahtarımız
* Ürettiğinden tekrar yeni anahtar üretirsin

Simetrik şifrelemenin çalışma modları nelerdir? Output feedback ve counter modu karşılaştırnız?

-Electronic Code Book (ECB): message is broken into independent blocks which are encrypted. each block is a value which is substituted, like a codebook.

-Cipher Block Chaining (CBC): message is broken into blocks, linked together in encryption operation. each previous cipher blocks is chained with current plaintext block



- Cipher Feedback (CFB): A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

-Output Feedback Mode (OFM)   
In output feedback mode, each block is dependent on the previous encryption, so each time a block is changed all the blocks should be re-encrypted from the start. Counter method solves this problem since each block is independently encrypted. But requires a synchronous counter and if the synchronization is lost, recovery of plaintext is erroneous.

A computer screen shot of a computer screen

Description automatically generated

ciphertextle oynayıp sonucu değiştiremezsin. Öncekilerde cipheri değiştirip bir sonraki cipheri ekleyebilirsin.

A computer screen shot of a computer screen

Description automatically generated

cipheri değiştirip plaini değiştirebilirsin.

-Counter (CTR):

öncekinin sonrakiyle bağlantısı yok.   
parallelelisable.  
bloklara rastgele erişim.  
Hızlı ve güvenli.

A hand writing on a piece of paper

Description automatically generated

A screenshot of a computer

Description automatically generated

A white background with black text

Description automatically generated

A close-up of a white text

Description automatically generated

A white board with math equations and numbers

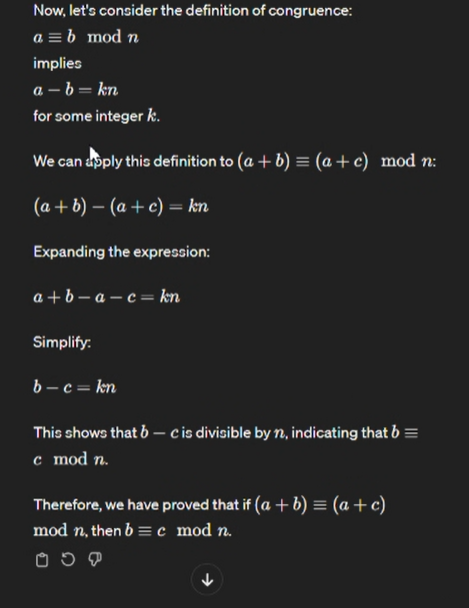
Description automatically generated

A close up of black text

Description automatically generated

A hand drawing a diagram on a piece of paper

Description automatically generated



A green line with a arrow pointing to the side

Description automatically generated

Risk: probability that a particular threat will exploit a particular vulnerability, probability of occurrence of security breach

risk analysis: process of identifying, assessing, and reducing risks to an acceptable level

evaluation

examination

quantitative

qualitative

risk management: planning, monitoring, controlling activities which are based on information produced by risk analysis activity

A close up of a text

Description automatically generated

3 aspects information security:

* security attack
* security mechanism
* security service
  + enhance security of data processing systems and information transfers of an organization

threat: the occurrence of which could have an undesirable impact on the well-being of an asset.

vulnerability: condition that has the potential to allow a threat to occur with greater frequency, greater impact or both

attack: assault on system security that derives from threat

Properties of Security Services

* authentication (iddia ettiğin kişi misin)
* access control
* data confidentiality
* authorization (yetkin var mı)
* data integrity
* nonrepudation

Assets to be protected

* information
  + confidentiality
  + integrity
  + availability
* resources
* prestige

A diagram of a diagram

Description automatically generated with medium confidence

security policy: a document stating security goals, which actions are required, which are permitted, which are allowed. Defines the way people interact with the data (who gets access, discussing information, printing, storing, etc.). Document that states in writing how a company plans to protect the company’s physical and information technology assets.

* standards / main rules
* users’ agreement
* procedures

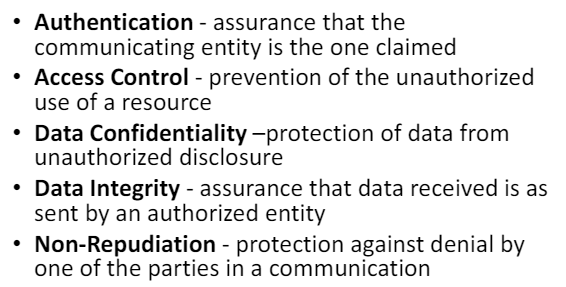
enforcement mechanism: firewall

what is network security policy? describe main properties of network usage policy

 **Network Security Policy:** A set of guidelines designed to protect an organization's network and data from threats such as unauthorized access and cyberattacks. It ensures the confidentiality, integrity, and availability of network resources.

 **Main Properties of Network Usage Policy:**

* **Access Control:** Defines who can access the network and to what extent.
* **User Authentication:** Ensures that only verified users access the network.
* **Data Protection:** Guidelines for protecting sensitive data.
* **Resource Usage:** Rules for acceptable use of network resources.
* **Incident Response:** Procedures for responding to security incidents.



İnkar Edememe (Non-repudiation): Bu prensip verinin iletildiği gönderici ve alıcı arasında ortaya çıkabilecek iletişim sorunları ve anlaşmazlıkları en aza indirmeyi amaçlar. İki sistem arasında bir bilgi aktarımı yapılmışsa ne gönderen veriyi gönderdiğini, nede alıcı veriyi aldığını inkar edememelidir.

differences between firewall and intrusion detection systems? what is firewall rules?

 **Firewall:** Monitors and controls incoming and outgoing network traffic based on predefined security rules to block unauthorized access.

 **Intrusion Detection System (IDS):** Monitors network traffic for suspicious activities and alerts administrators to potential threats.

* rule-based
  + anomaly – penetration identification
* statistical
  + threshold – profile based
* ---
* honeypots: decoy systems to lure attackers

 **Firewall Rules:** A set of conditions that define how a firewall should handle network traffic (allow, block, or log).

**Comparison of Symmetric and Asymmetric Cryptography:**

a. **Features, Generation, Encryption, Distribution, and Storing of Keys:**

* **Symmetric:** Uses a single key for both encryption and decryption. Key distribution can be challenging.
* **Asymmetric:** Uses a pair of keys (public and private) for encryption and decryption. Easier key distribution but more complex management.

b. **Speed of Methods:**

* **Symmetric:** Generally faster due to simpler algorithms.
* **Asymmetric:** Slower because of complex mathematical operations.

c. **Security of Methods:**

* **Symmetric:** Secure if the key is kept secret; vulnerable if the key is compromised.
* **Asymmetric:** Provides robust security; even if the public key is known, the private key remains secure.

d. **Application Fields:**

* **Symmetric:** Used in bulk data encryption, such as in file encryption and network traffic encryption.
* **Asymmetric:** Commonly used for secure key exchange, digital signatures, and encryption of small amounts of data.

e. **Implementation Characteristics:**

* **Symmetric:** Simpler to implement and computationally efficient.
* **Asymmetric:** More complex to implement and requires more computational resources.

which risk analysis method would you prefer for information security and why? explain the method and goals in detail.

**Explanation:** Quantitative risk analysis involves the use of numerical values to assess risks, typically by calculating the probability of an event and its potential impact.

**Goals:**

* **Objective Measurement:** Provides a precise and objective assessment of risks.
* **Financial Impact Estimation:** Helps in estimating the financial impact of security breaches, making it easier to justify investments in security measures.
* **Prioritization:** Allows for the prioritization of risks based on their quantified impact, facilitating better decision-making in resource allocation.

hash function and its main problem

A hash function is a mathematical algorithm that converts an input (or 'message') into a fixed-size string of bytes, typically a hash value. It is designed to be a one-way function, making it infeasible to reverse-engineer the original input from the hash value.

**Uses:**

* **Data Integrity:** Verifies that data has not been altered by comparing hash values before and after transmission or storage.
* **Digital Signatures:** Provides a secure way to sign documents and verify authenticity.
* **Password Storage:** Stores hashed versions of passwords to enhance security.

**Main Problem:** The primary issue with hashing is the potential for **collisions**, where two different inputs produce the same hash value, potentially compromising data integrity and security.

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

k = 0, 0, -1, … -254

keylen = 256

t[0] = 0, t[1] = 0, t[2] = -1, ….