SOLUTION

Instructions:

Attempt ALL questions completely and in sequence to get maximum points. There are 5 questions written on 2 pages. Do not write anything on the question paper. Return the paper by placing it inside your answer sheet.

Maximum Time Allowed: 180 Minutes (i.e. 3 Hours) **Maximum Points**: 50

Question #1: Write agree or disagree with a correct justification. You will NOT get any credit for providing vague answers, using any other term than AGREE or DISAGREE, and using AGREE and disagree both or disagreeing without correct justification. [CLO #1] **[1 x 20 = 20 points]**

i. Compression is a type of encryption technique used to change the size of data. Disagree. Not an encryption technique but to reduce data size
ii. RSA (Rivest-Shamir-Adleman) is a widely used symmetric encryption algorithm. Disagree Asymmetric Algorithm
iii. SHA-1 (Secure Hash Algorithm 1) is an example of a hash function which is used to produce a fixed-size output from a variable-size input. Agree
iv. Caesar cipher is an example of a transposition cipher and Rail fence cipher is an example of a substitution cipher. Disagree. Vice versa is true because rail fence has transposition and Caesar has substitution.
v. The purpose of ransomware is to provide free software. Disagree To encrypt files and demand payment for their release
vi. Worm is designed to spread from one computer to another without user intervention. Agree
vii. There is no role of a firewall in the context of malware defense. Disagree To filter and block unauthorized network traffic
viii. Encryption has no role to play in defense against industrial espionage. Disagree It prevents unauthorized access to data
ix. SQL injection can lead to unauthorized access, data manipulation, or deletion. Agree
x. The significance of the "LIMIT" clause in SQL injection attacks that it specifies the maximum length of injected code. Disagree It limits the number of rows returned by a query
xi. Complete online anonymity is good for security and has no drawbacks. Disagree Harmful actions become difficult to detect.
xii. The role of cookies in online privacy is to store information about user preferences and browsing history. Agree
xiii. Cross-Site Scripting (XSS) is an attack that primarily targets network infrastructure. Disagree Web application users
xiv. Cross-Site Request Forgery (CSRF) is a type of web application attack involves flooding a server with an overwhelming amount of traffic to disrupt its normal functioning. Disagree DDoS is that web application attack.
xv. Same-Origin Policy (SOP) is a common defense mechanism against web application attacks. Agree
xvi. Cyber Terrorism is an international collaboration for cybersecurity. Disagree The use of cyber attacks to create fear and panic for political or ideological purposes
xvii. Disinformation contributes to Information Warfare by promoting accurate and truthful information. Disagree By manipulating information to deceive and mislead
xviii. The term "volatile data" refer to in digital forensics means the data that is easily deleted in the system's memory such as process information. Agree
xix. Configuration file is an example of user-created file as a source of potential evidence in digital forensics. Disagree Computer-Created Files
xx. Authorized is one of the five basic rules of evidence in digital evidence collection. Disagree Understandable, admissible, authentic, reliable and complete are 5 basic rules.

Question #2: [CLO-2] **[2.5 x 3 = 7.5 points]**

a. Illustrate the difference between stream and block cipher using block diagrams. Give one example (name) of cipher in each case.

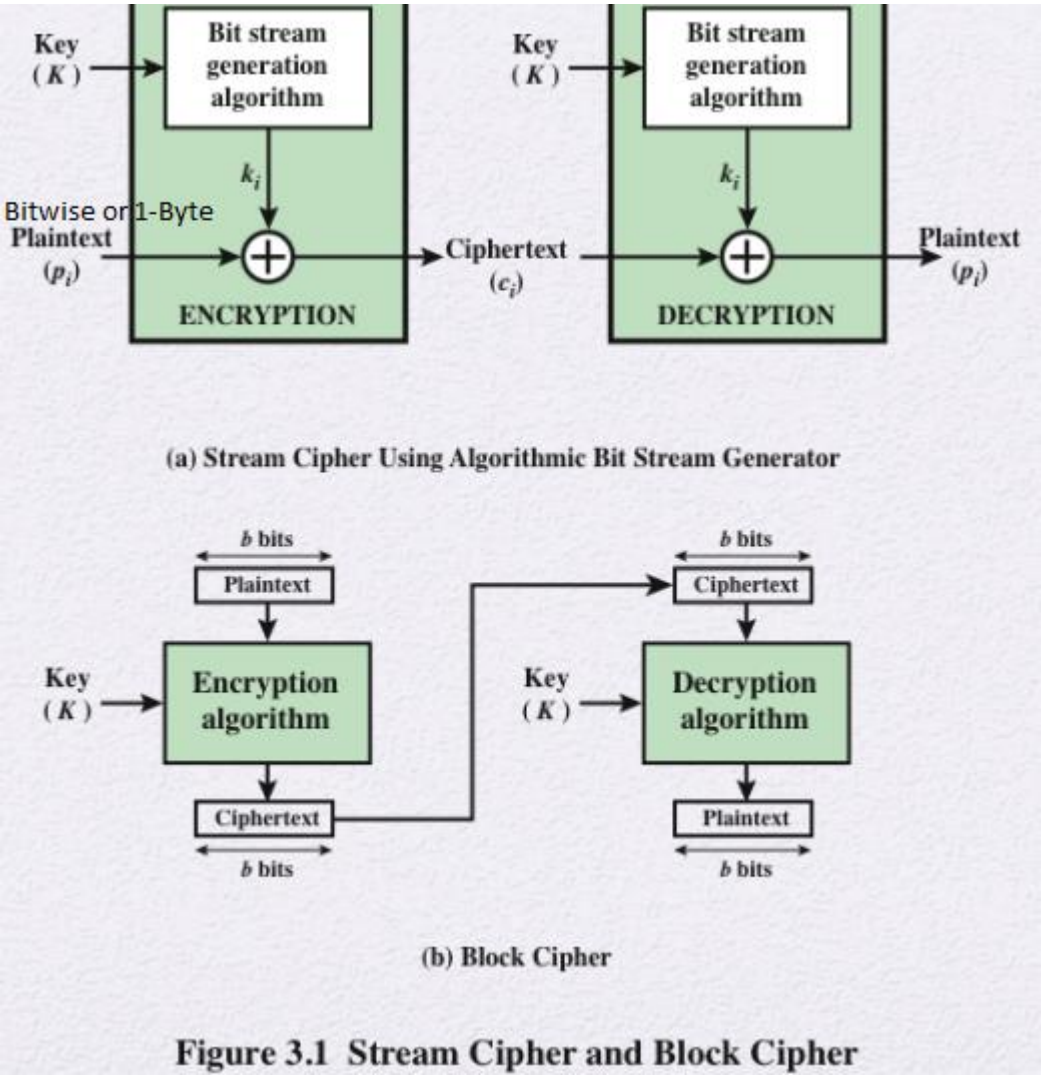


Figure 3.1 Stream Cipher and Block Cipher

Example Vernam Cipher (Stream Cipher) and DES or RSA etc (Block Cipher)

b. Apply RSA algorithm to find the public and private key pair using ***p = 5; q = 11; e = 3; M = 9*** where ***p*** and ***q*** are initial prime numbers. Use ***M*** as a plaintext to generate the ciphertext. Calculate the plaintext again using the generated ciphertext.

Solution

$n = p \times q = 5 \times 11 = 55$

$\varphi(n) = (p-1) \times (q-1) = 4 \times 10 = 40$

$\gcd(\varphi(n), e) = \gcd(40, 3) = 1$

$\because d \equiv e^{-1} (\mod \varphi(n))$

$d \times e \bmod \varphi(n) = 1$

$3d \bmod 40 = 1$

$\therefore d = 27$

So: Public Key $pu = \{e, n\} = \{3, 55\}$

Private Key $pr = \{d, n\} = \{27, 55\}$

Encryption:

$C = M^e \bmod n = 9^3 \bmod 55 = 14$

Decryption:

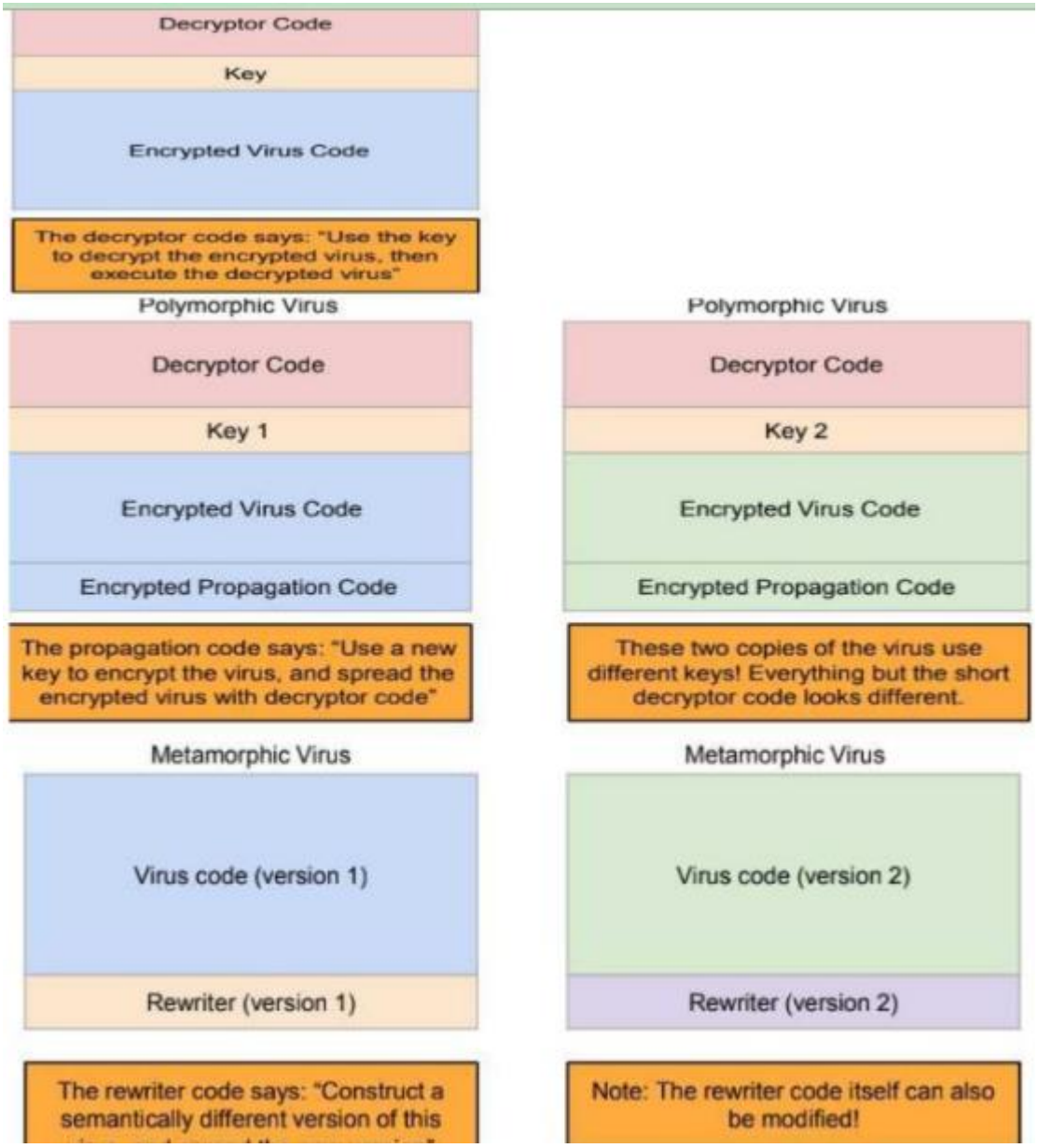
$$M = C^d \bmod n = 14^{27} \bmod 55 = 9$$

c. You are conducting a workshop where you need to explain a hash function. Discuss how would you describe its six properties?

1. **Arbitrary length input → fixed-length output –**
2. **Deterministic: you always get the same hash for the same message**
3. **One-way function (pre-image resistance, or hiding)**
   Given H, it should be difficult to find M such that H=hash(M)
4. **Collision resistant**
   Infeasible to find any two different strings that hash to the same value:
   Find M, M' such that hash(M) = hash(M')
5. **Output should not give any information about any of the input**
   Like cryptographic algorithms, relies on diffusion
6. **Efficient**
   Computing a hash function should be computationally efficient

Question #3: [CLO-2] [2.5 x 3 = 7.5 points]

a. Illustrate the polymorphic and metamorphic code with the help of suitable diagrams discuss two defense mechanisms in each case.



Defense against polymorphic code:

Strategy #1: Add a signature for detecting the decryptor code
○ Issue: Less code to match against → More false positives
○ Issue: The decryptor code could be scattered across different parts of memory
Strategy #2: Safely check if the code performs decryption
○ Execute the code in a sandbox
○ Analyze the code structure without executing the code
○ Issue: Legitimate programs might perform similar operations too (e.g. decompressing ZIP files)
○ Issue: How long do you let the code execute? The decryptor might only execute after a long delay.
Defense against metamorphic code:
● Behavioral detection
○ Need to analyze behavior instead of syntax
○ Look at the effect of the instructions, not the appearance of the instructions
○ Antivirus company analyzes a new virus to find a behavioral signature, and antivirus software analyzes code for the behavioral signature
● Subverting behavioral detection
○ Delay analysis by waiting a long time before executing malcode
○ Detect that the code is being analyzed (e.g. running in a debugger or a virtual machine) and choose different behavior
○ Antivirus can look for these subversion strategies and skip over them
• Flag unfamiliar code

b. Your business has a threat of internal espionage. Discuss five ways to lessen risk of internal espionage.
Give out data on a "need-to-know" basis.

Ensure no one person has control over all critical data at one time.

Limit portable storage media and cell phones. No documents/media leave the building.

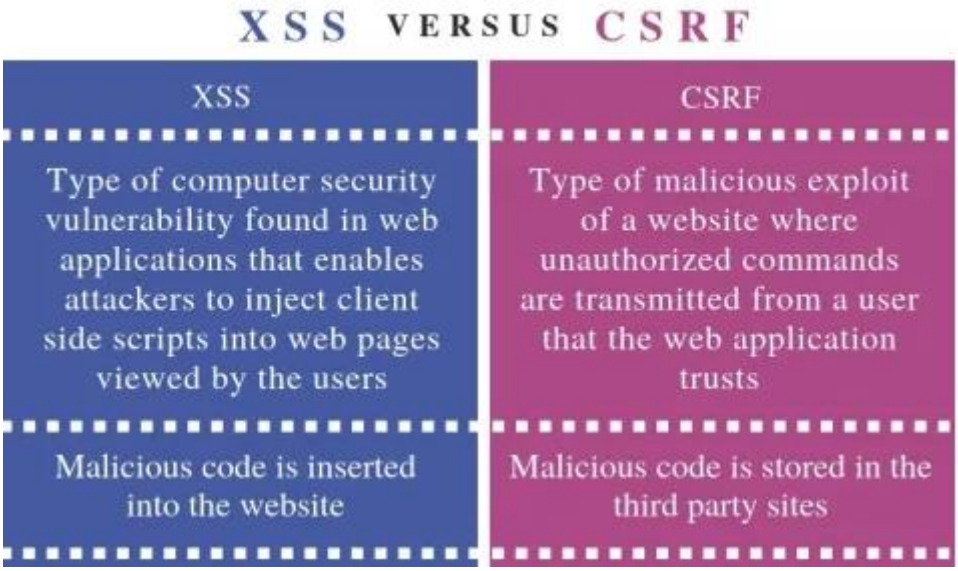
Do employee background checks.

Scan PCs of departing employees.

Lock up tape backups, documents, and other media.

Encrypt hard drives of portable computers.

c. Differentiate between cross-site scripting (XSS) & cross-site request forgery (CSRF). Write at least 2 clear differences.



Question # 4: **[CLO-3]** **[2.5 x 3 = 7.5 points]**

a. Explain how SQL injection attack can be launched in the following URLs and SQL queries by providing one example in each case:

i. https://iamnotsecure.com/products?category=Bags
Use OR 1=1

ii. SELECT * FROM users WHERE username = 'ali123' AND password = 'happiness';
Use – -- (hyphen) after username field

iii. A piggybacked SQL query Use DROP TABLE query

iv. Inserting an unauthorized user into a database INSERT INTO query example (complete)

v. Using UNION keyword and retrieving all usernames and passwords UNION plus SELECT query complete with UID and PWD

b. The following diagram (Figure 1) is an example of cascaded authorization. Suppose that at time t =45, Ali revokes the authorization given to Chaman. Draw the final diagram after revocation and discuss the solution.

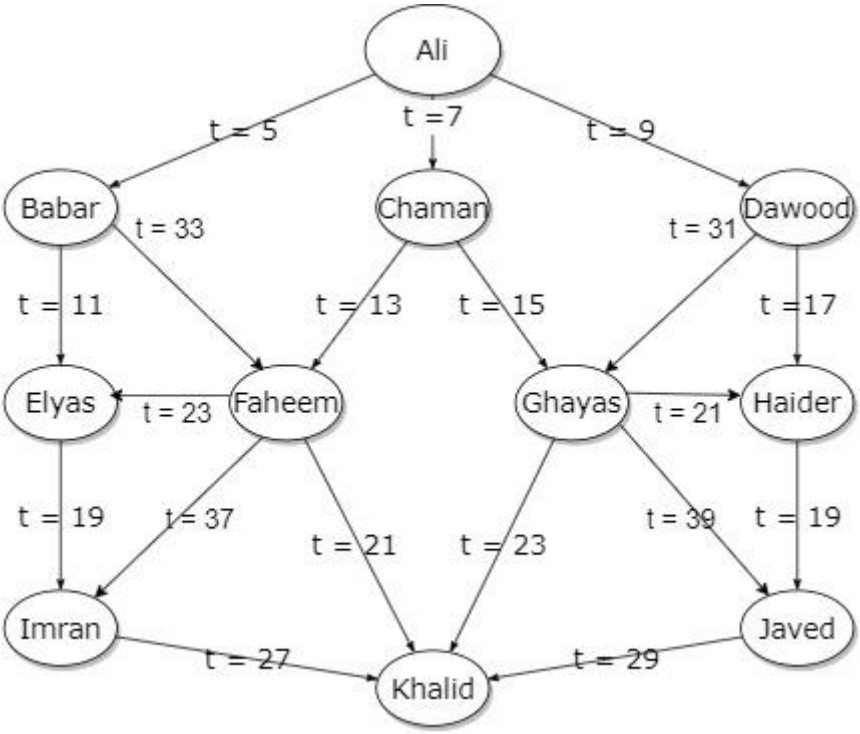
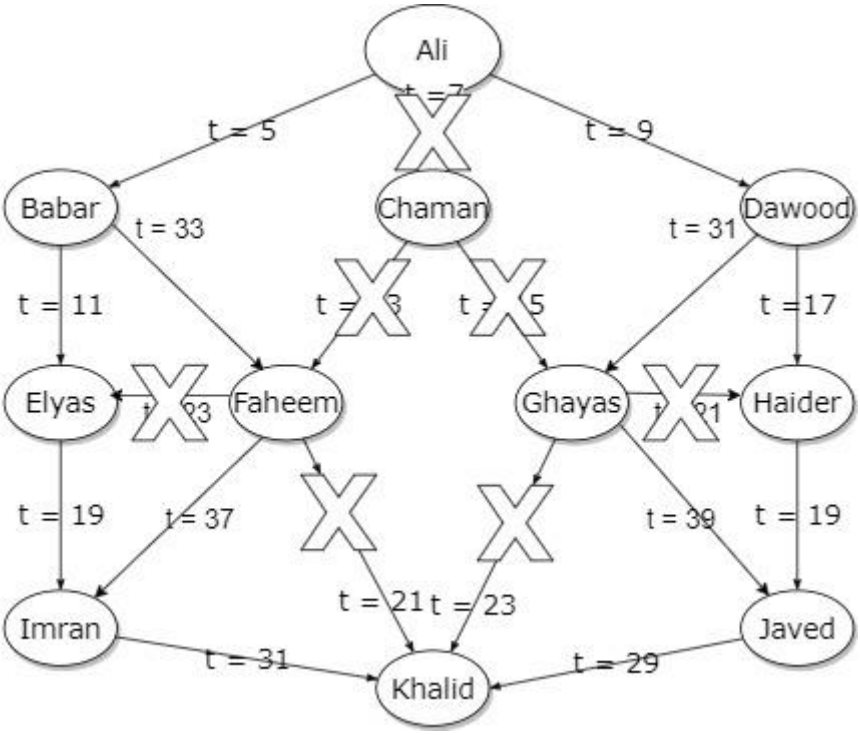


Figure 1: Cascaded Authorization

Solution:
Explanation with following result



c. Use the following dataset (Table 1) to make it anonymous for k = 3 (if possible). State not possible otherwise.

Table 1
Dataset without k-Anonymity

Name	Age	Postal Code	Gender	Disease
Bella	53	100-110	Female	Cirrhosis
Naomi	39	100-101	Female	Cancer
Ian	45	100-053	Male	Obesity
Liam	21	100-067	Male	Polyneuropathy
Eva	19	100-009	Female	ADHD
Gina	26	100-114	Female	Chronic Bronchitis
Jack	87	100-033	Male	Ulcer
Paul	72	100-021	Male	Stroke

Solution: (sample) yours may differ slightly

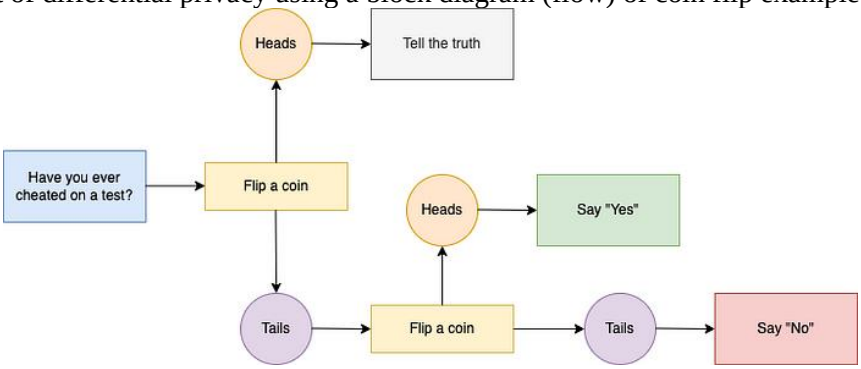
One may also say it is not completely possible for k=3.
OR

Table 2
Dataset with k-Anonymity

Name	Age	Postal Code	Gender	Disease
*	50-59	100-***	*	Cirrhosis
*	30-39	100-***	Female	Cancer
*	40-49	100-***	Male	Obesity
*	20-29	100-***	*	Polyneuropathy
*	10-19	100-***	*	ADHD
*	20-29	100-***	Female	Chronic Bronchitis
*	80-89	100-***	Male	Ulcer
*	70-79	100-***	Male	Stroke

Question# 5: [CLO-3] [2.5 x 3 = 7.5 points]

a. Illustrate the concept of differential privacy using a block diagram (flow) of coin flip example.



b. In January 2021, the Pakistani banking sector suffered a massive cyber-attack that resulted in the loss of millions of dollars. This attack highlights the critical need for stronger cybersecurity measures in the country. Suggest security improvements needed to be taken by the following:

i. Individuals or General Population **ii.** Banks and Businesses **iii.** Government

Solution:

One of the measures is to increase **awareness among the general population** about cybersecurity. This can be achieved through education and training programs that teach individuals about basic cybersecurity measures and how to protect themselves against cyber threats.

Another opportunity is for **businesses to invest in cybersecurity infrastructure and expertise**. Investing in cybersecurity can help protect businesses from financial and reputational damage caused by cyber-attacks. It can also help them gain a competitive advantage by demonstrating to their customers that they take cybersecurity seriously.

Finally, the Pakistani **government can take steps to strengthen cybersecurity laws and regulations**. The government can work with industry experts to develop and implement stronger cybersecurity laws that provide better protection against cyber threats. This will help create a more secure digital environment for businesses and individuals in Pakistan.

c. Sameer is the managing director of a respected software company. After finding illegal & pirated software downloaded on his network server and several individual office computers, he decided to hire a computer forensics investigator to build a case for employee dismissal. The Investigator was hired to locate deleted files if any, locate spy software, detect illegal file-sharing software & verify certain non-work-related contents of the hard drives in question. All this evidence must be collected using some defined rules discussed in the class lectures. Discuss them.

Digital evidence collection must be governed by five basic rules that make it admissible in a court of law:

Understandable
Evidence must be clear and understandable to the judges

Admissible
Evidence must be related to the fact being proved

Authentic
Evidence must be real and appropriately related to the incident

Reliable
There must be no doubt about the authenticity or veracity of the evidence

Complete
The evidence must prove the attacker's actions or his/her innocence