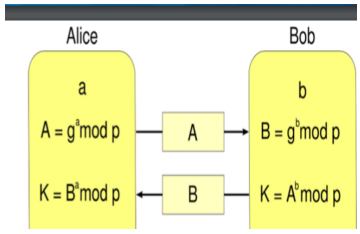
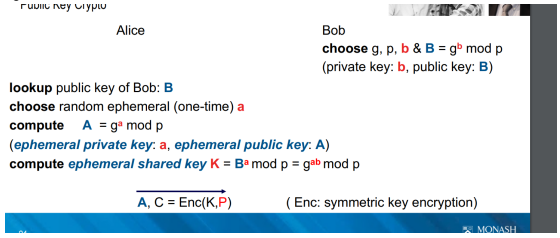
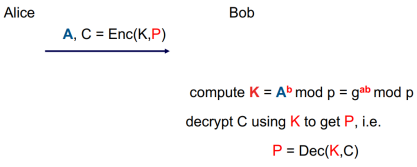
Software Security:format A potential vulnerability that should be checked is{1.Type of vulnerability}. (why this is a vulnerability)This is especially important because {}. This means that without{protection mechanism防御方法}, if an attacking user {攻击输入}, it will {软件怎样运行攻击输入} and potentially cause {被攻击的后果（如密码被盗）}. To test for this vulnerability, one way {测试方法，同攻击方法} instead of {正常输入} and see if it gets executed and produces the expected output. Another way (with access to the app code) is to analyse the code and see what if any validation checks it makes on the input file.
Database Security::format To achieve {n}-anonymity using the {generalisation/ Cell suppression/Noise addition} protection operation on {column(s)}, we need to ensure at least {n} identical rows exist in the view for every possible generalised value for {column1,column2….} pairs. One way to achieve this without losing all information is: for {column1}, {operation only reveal the category among e.g. (1940-1969, 1970-1989, 1990-2009)}, and for{column2} {operation: only reveal the category among (Theft/Burglary, Murder/Manslaughter)}. It gives the following {cell suppressed/generalised/noise added} view, showing that {n}-anonymity is satisfied.
But {n}-diversity for residence {is/not} satisfied by this protection method, {reason:e.g.since both criminals born in 1970-1989 committing Murder/Manslaughter reside in Melbourne and both criminals born in 1970-1989 committing Theft/Burglary reside in Sydney. }
Web Security/Security Protocols:format:Attack 1 (SQLi):a. type: active/passive; violated security property: {confidentiality/integrity/authenticity/availability} . Attack 2 {same as attack1} b.{type of attack} {attacking steps}

unconditionally secure cipher and computationally secure
Math:
(c + d) mod n ≡ (c mod n + d mod n) mod n
Calculation:
(5 * 14) mod 12 ≡(5 mod 12 * 14 mod 12) mod 12 • a = 5, n = 7: b = 5^-1 mod 7 = 3 • check: 5 x 3 mod 7 = 15 mod 7 = 1
Euler's Theorem: If M and n are relatively prime, then ○ M^ø(n) mod n = 1 Fermat's Little Theorem: If p is a prime number and M is relatively prime to p, then ○ Mø(n) mod p = M^(p–1) mod p = 1
7^5 mod 11 (a = 7, e = 5, n = 11),e = 510 = 1012 • Start from Most Significant (leftmost) bit of e (always 1), set z = a. • For each subsequent bit bi of e: • If bit bi = 0, just square z, i.e. set z = z2 mod n • If bit bi = 1, square z and multiply it by a,
i.e. set z = z2 x a mod n • 75 mod 11 example: • Start with MS bit b2=1 of e = 1012 , set z = a = 7. • I = 2: bit b1 = 0 à square: z = z2 mod n = 72 mod 11 = 5 • i = 1: bit b0 = 1 à square & multiply: z = z2 x a mod 11 = 52 x 7 mod 11 = 3 x 7 mod 11 = 10
104 mod 3 = (10 mod 3)4 mod 3
Public key encryption
Diffie hellman

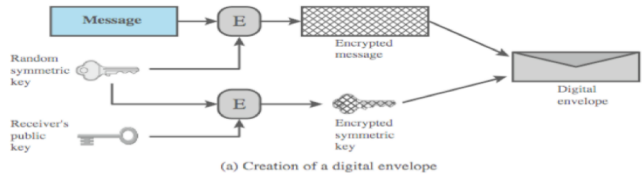


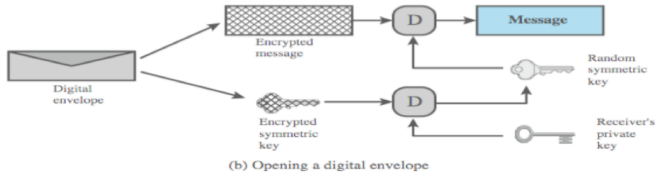
Elgamal

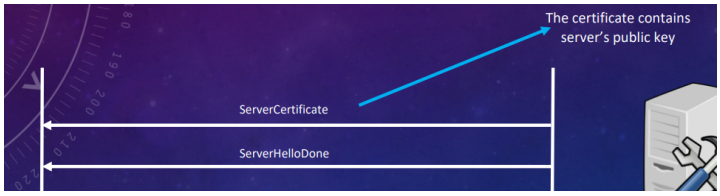


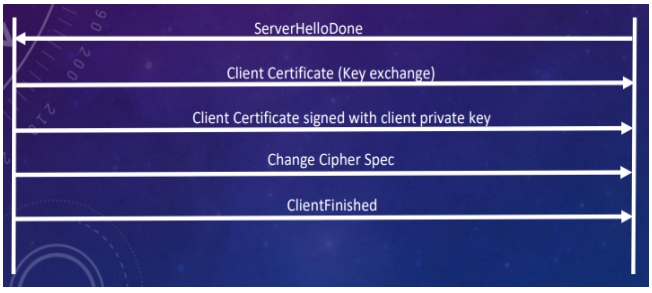


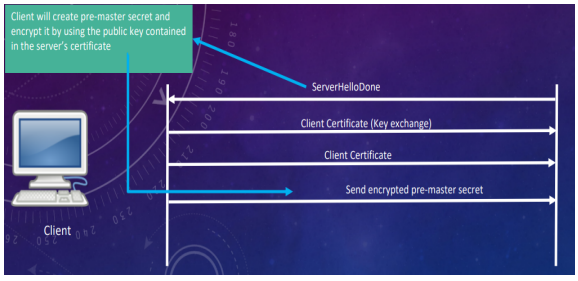
Can an MITM attack apply for elgamal? Explain your reasons. Assuming that Bob's public key B is hosted at a secure server, that allows Alice to lookup, then B cannot be replaced. However since Alice's ephemeral public key A is sent together with the ciphertext, it is possible for this A to be changed. Thus, when Bob receives the modified A, the key K that he computes will differ from what Alice would compute. What is worse is that the attacker will also be able to compute this key.
Hybrid encryption:

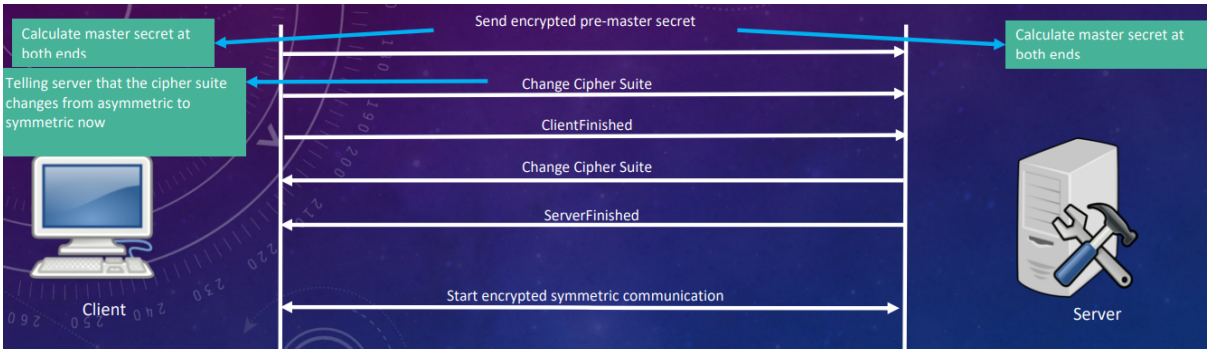












Rsa

• choose two distinct large primes p and q • compute the modulus n = pq • compute the Euler's totient function ø(n) = (p–1)(q–1) • choose an integer e coprime to ø: e is the public key • compute d = e^–1 mod ø(n) as e's inverse: d is the private key • Note: e×d ≡ 1 mod ø(n) since d is the multiplicative inverse of e

● choose two primes: p = 5, q = 11 ● compute the modulus n = p x q = 55 ● compute ø(n) = (p–1) x (q–1)= 4 x 10 = 40 ● find out two numbers e = 3 & d = 27 which satisfy (3 * 27) mod 40 = 1

• c = me mod n • m = cd mod n

Mac

What are three requirements for MAC? (a) Knowing a message and MAC, it is computationally infeasible to find another message with same MAC (b) MACs should be uniformly distributed across the messages (c) MACs should depend equally on all bits of the message

Tls

TLS sits between the application layer and the transport layer.

3. What is the role of ChangeCipherSpec message in TLS record protocol? It triggers the record protocol to start encrypting the traffic using negotiated keys and algorithms. The ChangeCipherSpec must be sent by both sides (client and server) for TLS record protocol to start encrypting the traffic.

IPsec operates at which layer of TCP/IP protocol stack? Network layer

7. What is the difference between Tunnel mode and Transport mode of ESP? In transport mode, AH and ESP provide protection primarily for next layer protocols; in tunnel mode, AH and ESP are applied to tunneled IP packets

9. Explain the purpose of the numeric comparison or passkey entry association models in the Bluetooth LE Secure Connections protocol. The purpose is to allow the two devices A and B that intend to communicate securely to verify via an authenticated channel (i.e. via the human user) that they are really talking to each other, to prevent Man-In-The-Middle (MITM) attacks where A and B are each talking in two separate sessions to an attacker M rather than to each other. For example, for numeric comparison model, in the case of the MITM attack, the number displayed at device A (which is derived from the shared of key of M with$A$) would not match the number displayed at device B (which is derived from the shared key of M with B) so the numeric comparison will fail.

week7

o Authentication Protocol:
User sends identity to host
host responds with challenge x (random / current time)
User's token computes and sends back response y = f(x,K)
host compares y from user with own computed f(x,K), if match user authenticated
- protects against eavesdropping and replay threats

Application of MAC to Challenge-Response user authentication
- Solution: To make a secure protocol against eavesdropping attacks, use a secure MAC o Verifier sends random challenge "message" x
o Prover responds with R = MAC(K, x)
o Verifier checks if R = MAC(K, x)
o Protocol is secure against eavesdropping if MAC is existentially unforgeable under chosen message attack and x is suff. long to avoid x repeats (e.g. 256 bit).
- MAC challenge-response Variant 1:
o Challenge x may be time of day instead of random
o Advantage: Using synchronised clocks, no need for explicit challenge message to be transmitted Application of digital signatures to Challenge-response user authentication
- Problem with MAC-based challenge-response protocol:
o Verifier Server needs to store shared key K
o What if hacker exposes Server's stored key K?
- Solution: Replace MAC with a digital signature
o Setup: prover generates sk, sends pk to verifier.
- Protocol:
o Verifier sends random challenge "message" x
o Prover responds with y = Sign(sk, x)
o Verifier checks if y is a valid signature on x with respect to prover's public key pk
- Protocol is secure against eavesdropping if signature is existentially unforgeable under chosen message attack and x is suff. long to avoid x repeats (e.g. 256 bit).

Multifactor User Authentication
- Multifactor authentication: combine more than one authentication method to improve security: - Attacker needs to compromise all used factors to attack the system
- reduce likelihood of successful attack
- E.g. common combination:
- Something you know (password) +
- Something you have (token)

Week 8 – Access Control

Access Control Principles

- Definition: "The prevention of unauthorised use of a resource, including the prevention of use of a resource in an unauthorised manner"
- central element of computer security
- assume have users and groups
o authenticate to system
o assigned access rights to certain resources on system

Access Control Elements
- subject - entity that can access objects
o a process representing user/application
o often have 3 classes: owner, group, world
- object - access controlled resource
o e.g. files, directories, records, programs etc
o number/type depend on environment
- access right - way in which subject accesses an object
o e.g. read, write, execute, append, delete, create, search

What do we mean by access control?
- Rules that define which subject can access what object
- Q: What does the term ACCESS mean with respect to information resources?
- normally read, write, execute
- e.g. Unix OS uses these operations
- The file owner can control the permissions to these operations.
- Windows OS has, in addition to these, permissions for delete, change ownership and change permissions - Some systems define write that includes reading rights. These systems often have one more operation à append (blind write)

Access Control Types:

IDiscretionary Access Control (DAC)

- Controls access based on the identity of the requestor and on access rules on what requestors are allowed/not allowed to do.
- termed discretionary because an entity might have access rights that permit the entity, by its own volition, to enable another entity to access some resource.
· Mandatory access control (MAC)
- Controls access based on comparing security labels (sensitivity of resources) with security clearances (eligibility of entities to access certain resources).
· Role-based access control (RBAC)
- Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles.

Discretionary Access Control
- Access to information is controlled by the owner of the object
- It can also provide for centralised or distributed security management
- Centralised security — an administrator provides and controls access
- Distributed security — managers or team leaders control access
- Commonly used Operating Systems (UNIX, Windows,…) implement this method of access control Mandatory Access Control
- Imposes universal security conditions for all users, IT systems and information
- Commonly used in military systems
- Information is classified based on attributes such as sensitivity, secrecy and confidentiality - A subject is said to have a security clearance of a given level;
- an object is said to have a security classification of a given level
- MAC also known as a Multilevel model
- Categorizes information by sensitivity and user access is based on their responsibility level - Security levels
- A hierarchy of sensitivity attributes (ordering of levels)
- Typical military-style hierarchy
- An object's sensitivity attribute is called classification
- Subjects have clearances to access objects in the hierarchy
- Dominates-relation: we say that x dominates y iff level(x) ≥ level (y)
- Allows: subjects x access to objects y accesstype à binary value

Role-Based Access Control
- Access to information and its resources is based on a user's role (role = group of users, one policy for all users in group)
- It can cater for hierarchies and business constraints