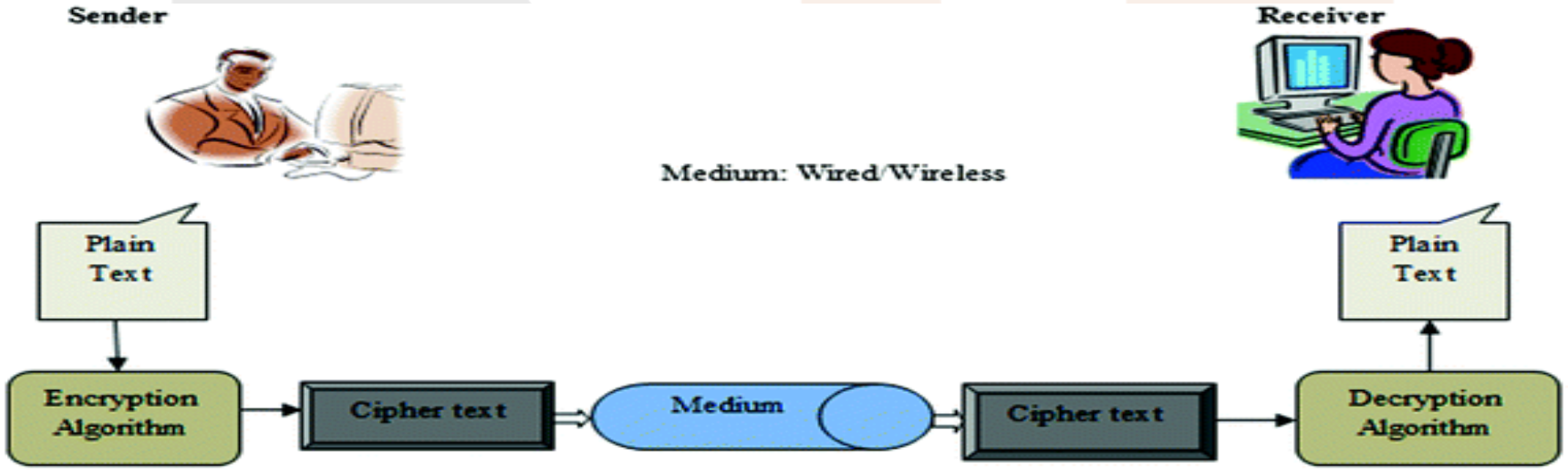
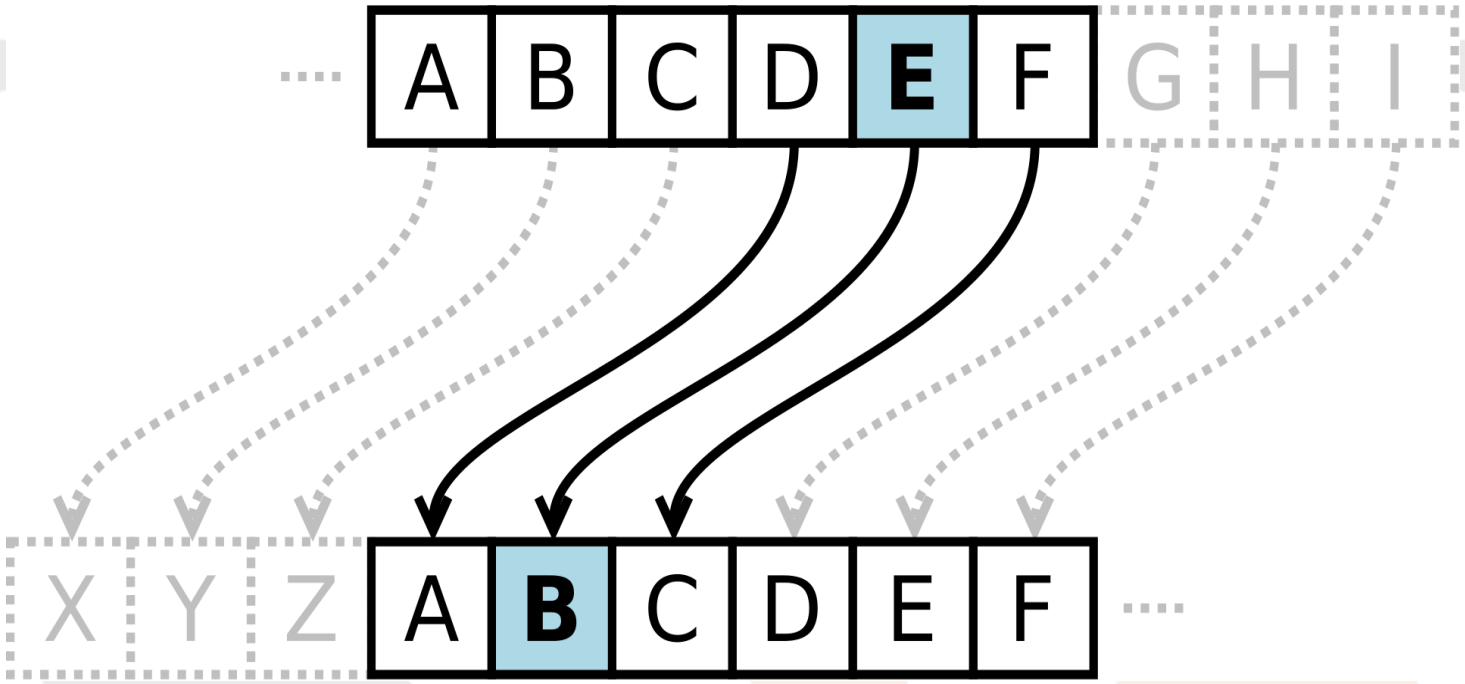
Cryptography

- **Cryptography**, (from Ancient Greek: *kryptós* "hidden, secret"; and *graphein*, "to write"), is the practice and study of techniques for secure communication in the presence of third parties called adversaries.
- More generally, cryptography is about constructing and analysing protocols that prevent third parties or the public from reading private messages; various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography.
- Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications.

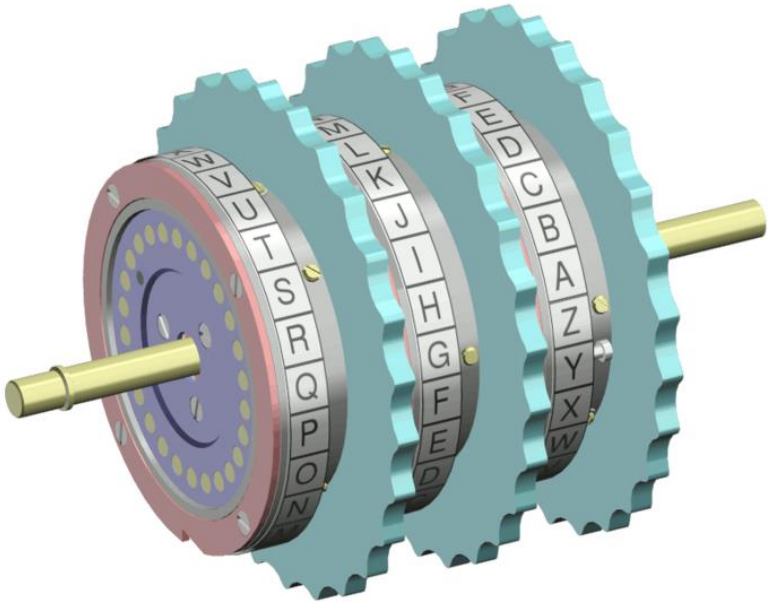


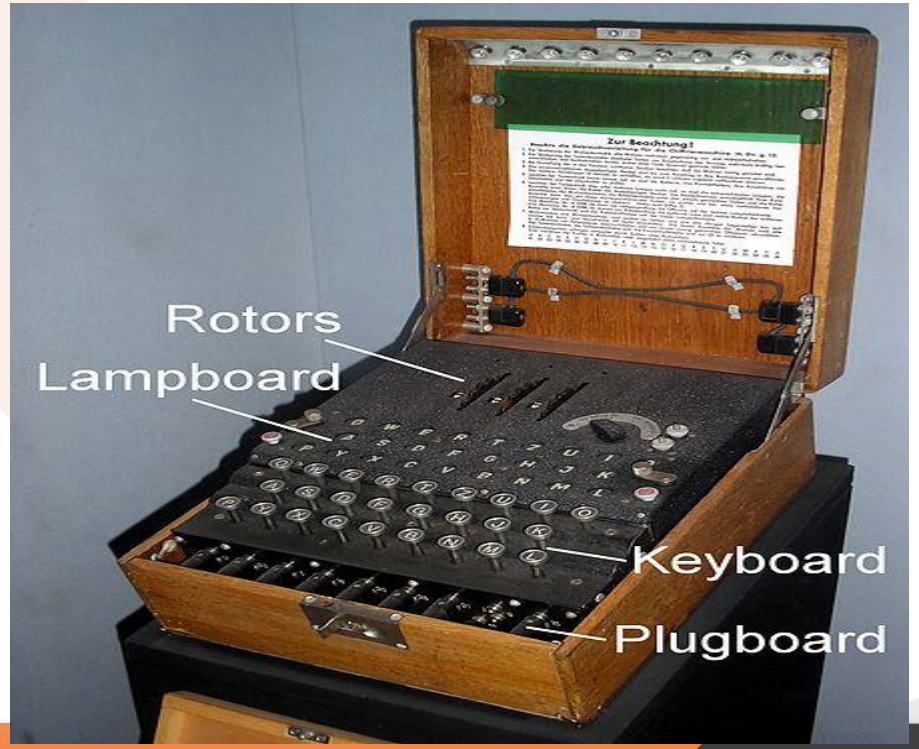


Alphabet shift ciphers are believed to have been used by Julius Caesar over 2,000 years ago.

16th-century book-shaped French cipher machine, with arms of Henri II of France

- Cryptography prior to the modern age was effectively synonymous with *encryption*, the conversion of information from a readable state to apparent nonsense. The originator of an encrypted message shares the decoding technique only with intended recipients to preclude access from adversaries.
- The cryptography literature often uses the names Alice ("A") for the sender, Bob ("B") for the intended recipient, and Eve ("eavesdropper") for the adversary.
- Since the development of rotor cipher machines in World War I and the advent of computers in World War II, the methods used to carry out cryptology have become increasingly complex and its application more widespread.



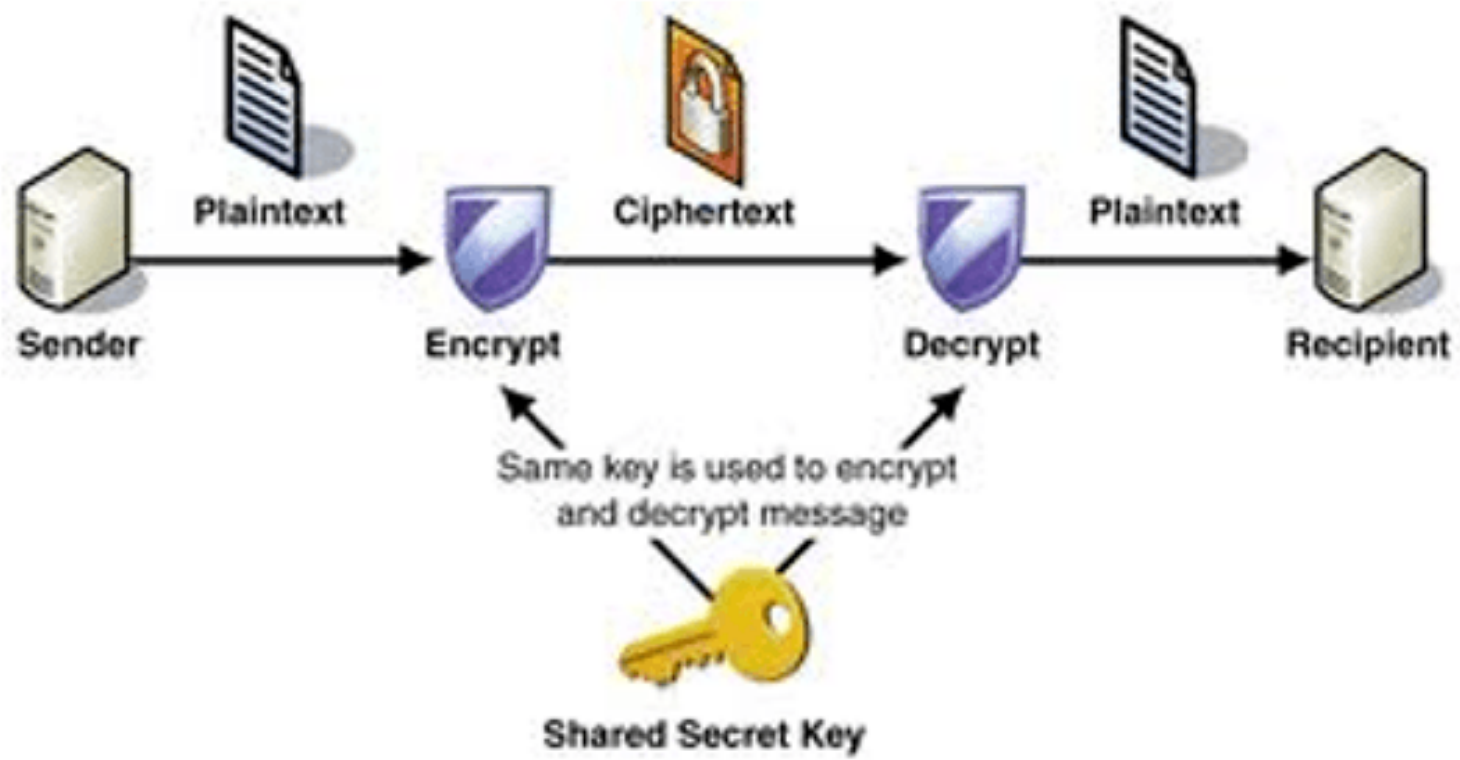


- Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary.
- It is theoretically possible to break such a system, but it is infeasible to do so by any known practical means. The growth of cryptographic technology has raised a number of legal issues in the information age.
- In some jurisdictions where the use of cryptography is legal, laws permit investigators to compel the disclosure of encryption keys for documents relevant to an investigation. Cryptography also plays a major role in digital rights management and copyright infringement of digital media.

Break

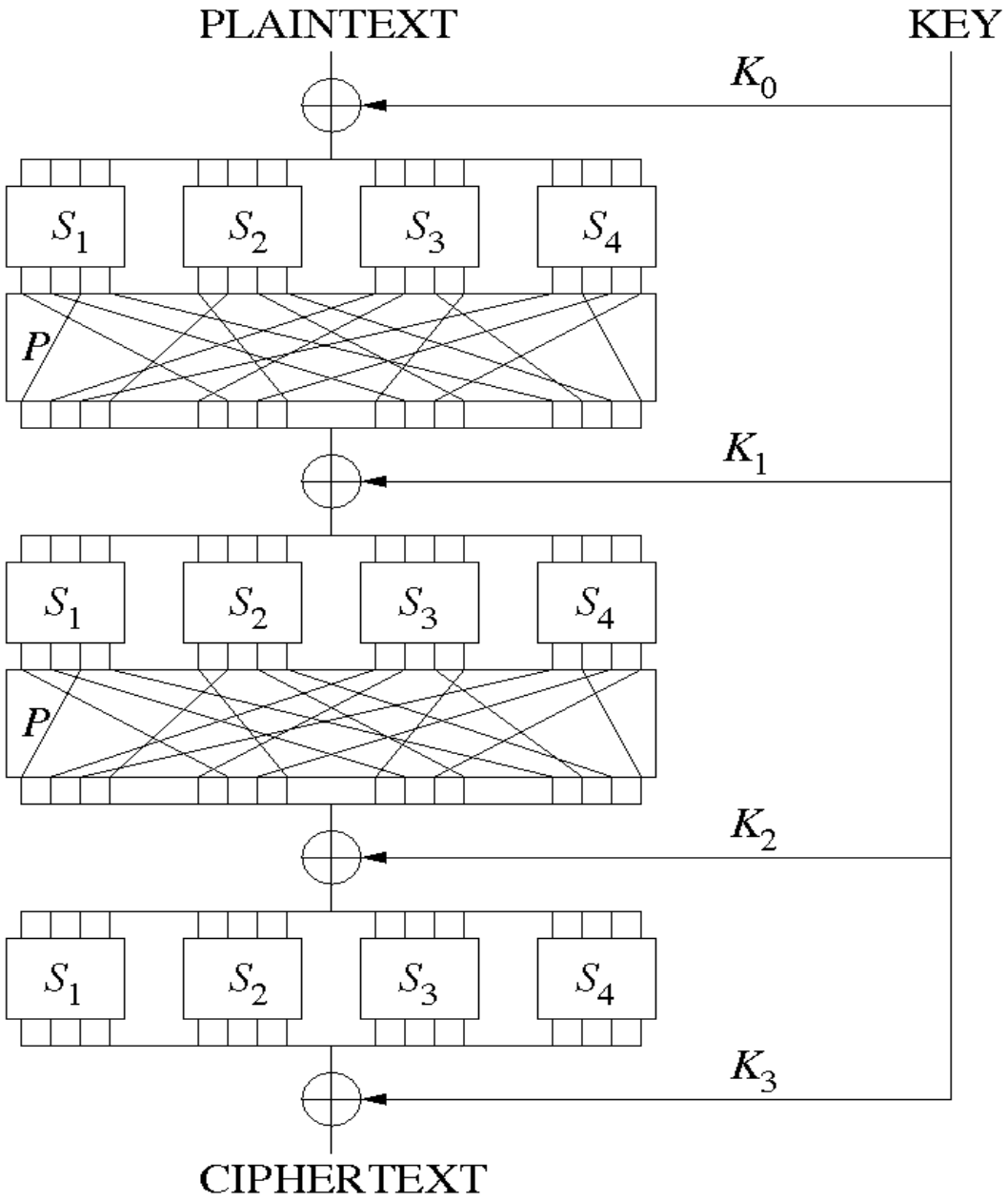
Symmetric key

- Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key (or, less commonly, in which their keys are different, but related in an easily computable way). This was the only kind of encryption publicly known until June 1976.



- The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are block cipher designs that have been designated cryptography standards by the US government (though DES's designation was finally withdrawn after the AES was adopted).

- Despite its deprecation as an official standard, DES (especially its still-approved and much more secure triple-DES variant) remains quite popular; it is used across a wide range of applications, from ATM encryption to e-mail privacy and secure remote access.



Q Consider the following two statements: **(GATE-2007) (1 Marks)**

i. A hash function (these are often used for computing digital signatures) is an injective function.

ii. encryption technique such as DES performs a permutation on the elements of its input alphabet.

Which one of the following options is valid for the above two statements?

(A) Both are false

(B) Statement (i) is true and the other is false

(C) Statement (ii) is true and the other is false

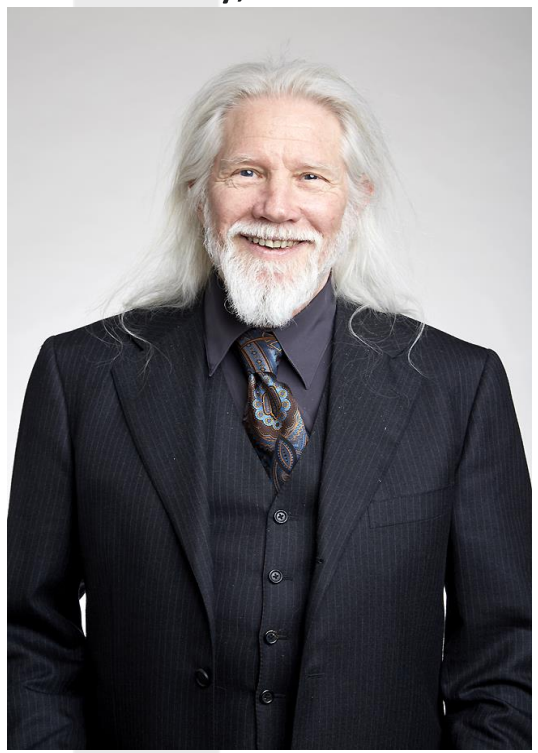
(D) Both are true

Break

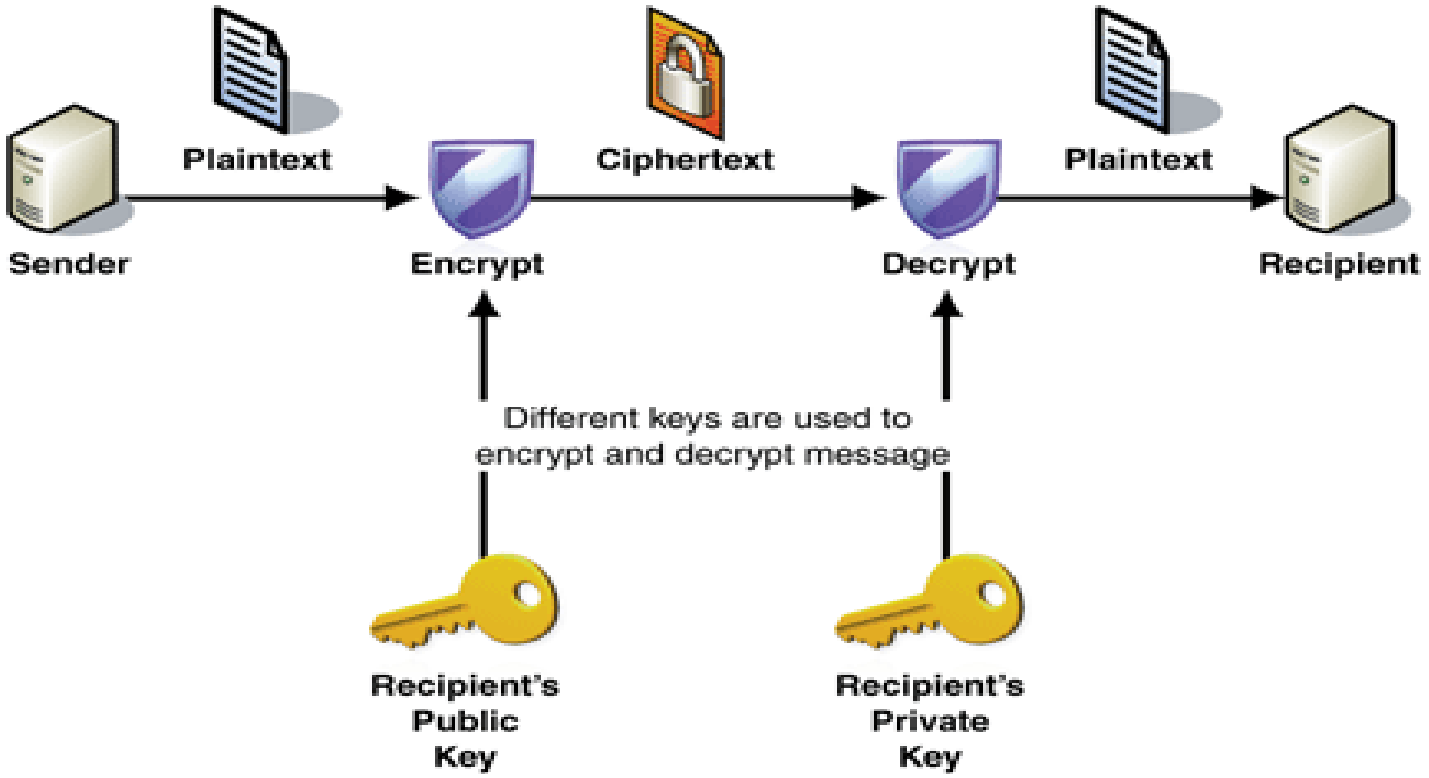
Asymmetric key (Public-key cryptography)

- Symmetric-key cryptosystems use the same key for encryption and decryption of a message, although a message or group of messages can have a different key than others.
- A significant disadvantage of symmetric ciphers is the key management necessary to use them securely. Each distinct pair of communicating parties must, ideally, share a different key, and perhaps for each ciphertext exchanged as well.
- The number of keys required increases as the square of the number of network members, which very quickly requires complex key management schemes to keep them all consistent and secret.

- In a ground breaking 1976 paper, Whitfield Diffie and Martin Hellman proposed the notion of *public-key* (also, more generally, called *asymmetric key*) cryptography in which two different but mathematically related keys are used—a *public* key and a *private* key.
- A public key system is so constructed that calculation of one key (the 'private key') is computationally infeasible from the other (the 'public key'), even though they are necessarily related. Instead, both keys are generated secretly, as an interrelated pair.



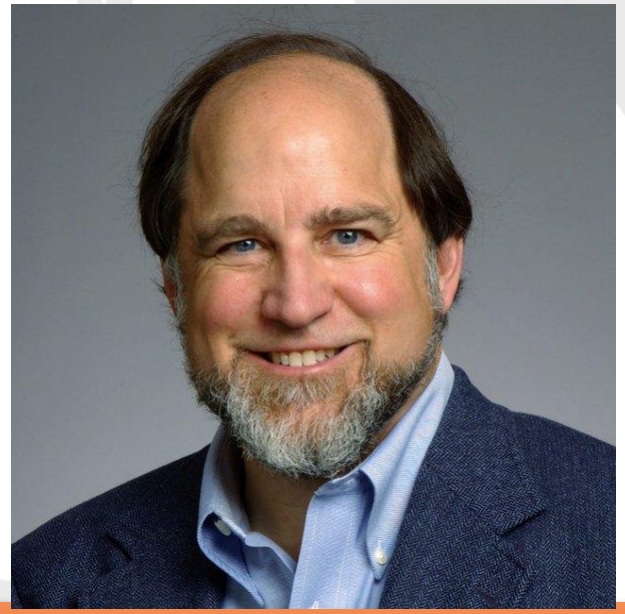
Whitfield Diffie

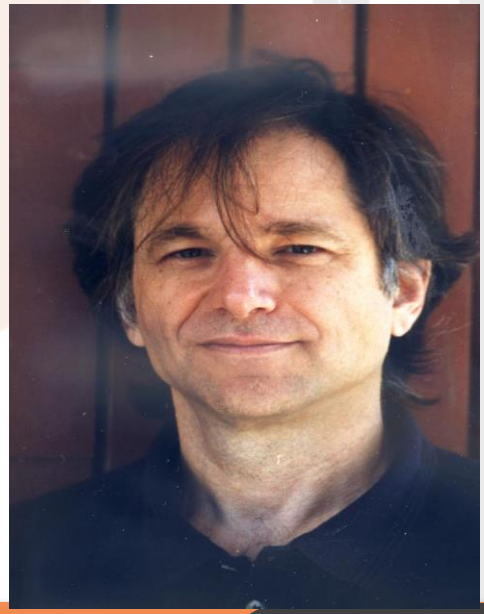


Martin Hellman

- In public-key cryptosystems, the public key may be freely distributed, while its paired private key must remain secret. In a public-key encryption system, the *public key* is used for encryption, while the *private* or *secret key* is used for decryption. While Diffie and Hellman could not find such a system, they showed that public-key cryptography was indeed possible by presenting the Diffie–Hellman key exchange protocol, a solution that is now widely used in secure communications to allow two parties to secretly agree on a shared encryption key.

- Diffie and Hellman's publication sparked widespread academic efforts in finding a practical public-key encryption system. This race was finally won in 1978 by Ronald Rivest, Adi Shamir, and Len Adleman, whose solution has since become known as the RSA algorithm.

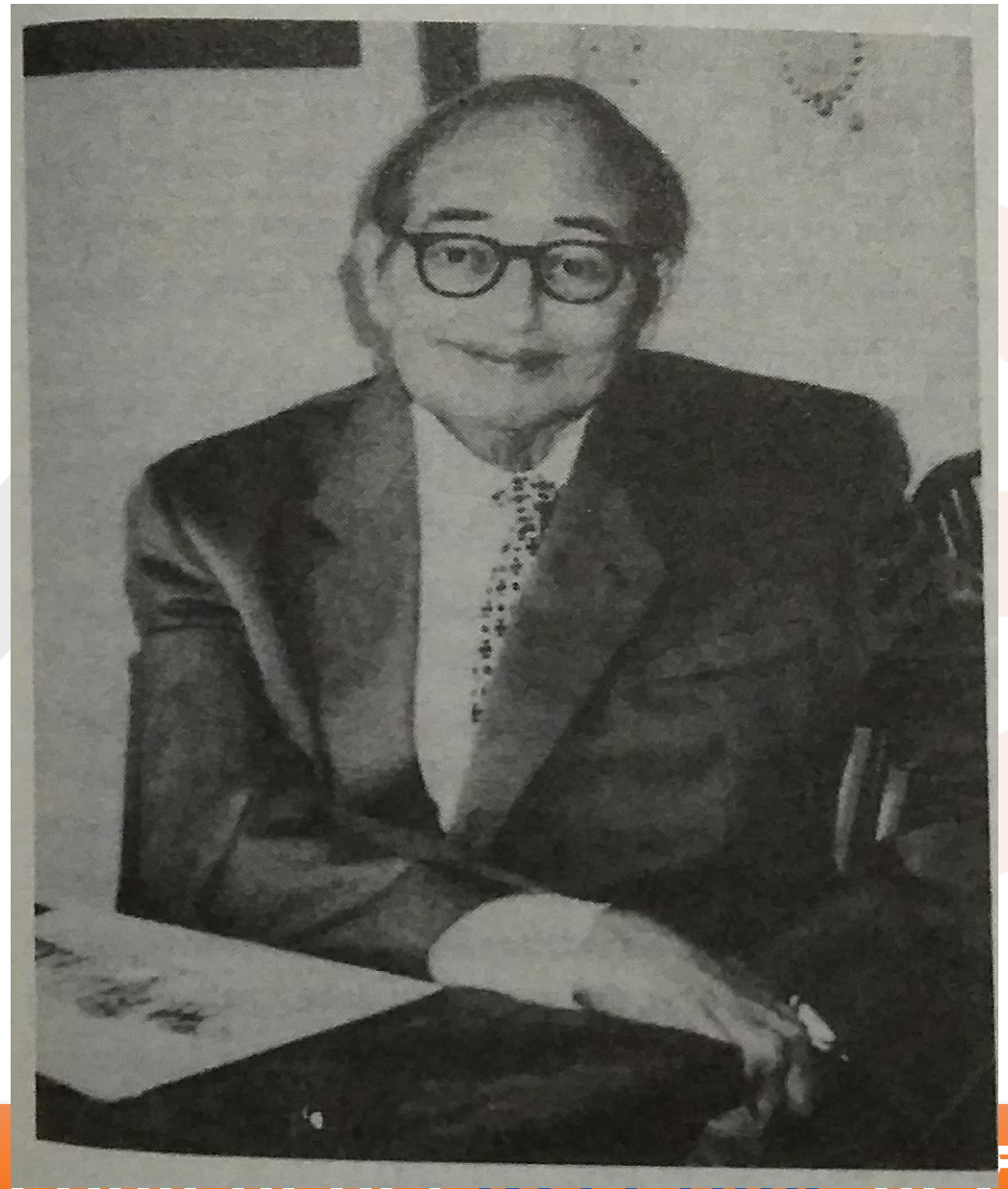




- The Diffie–Hellman and RSA algorithms, in addition to being the first publicly known examples of high quality public-key algorithms, have been among the most widely used.

- A document published in 1997 by the Government Communications Headquarters (GCHQ), a British intelligence organization, revealed that cryptographers at GCHQ had anticipated several academic developments.

- Reportedly, around 1970, James H. Ellis had conceived the principles of asymmetric key cryptography.

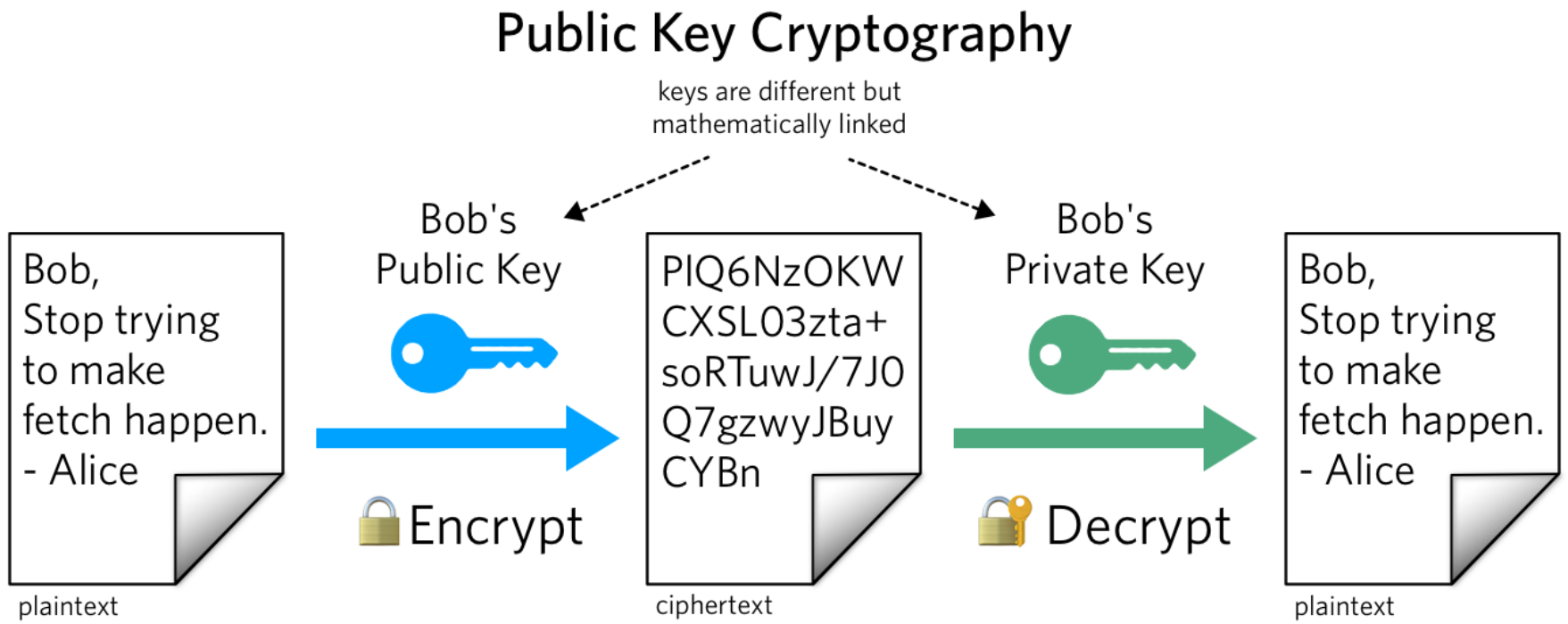


- In 1973, Clifford Cocks invented a solution that very similar in design rationale to RSA.

- And in 1974, Malcolm J. Williamson is claimed to have developed the Diffie–Hellman key exchange.

Break

Confidentiality

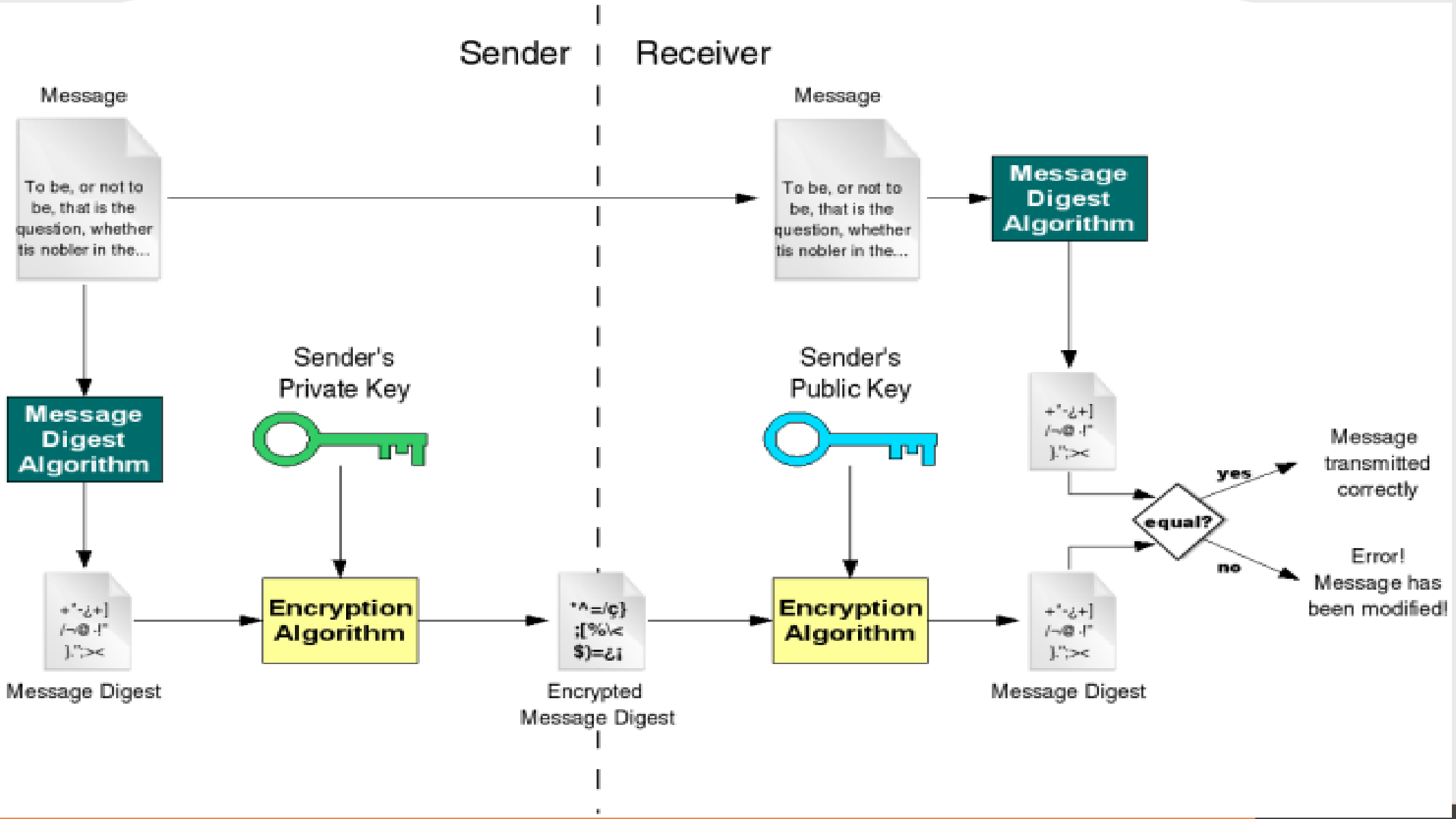


Q Suppose that everyone in a group of N people wants to communicate secretly with the N–1 other using symmetric key cryptographic system. The communication between any two persons should not be decodable by the others in the group. The number of keys required in the system as a whole to satisfy the confidentiality requirement is **(GATE-2015) (1 Marks)**

(A) 2N **(B)** N(N – 1) **(C)** N(N – 1)/2 **(D)** $(N - 1)^2$

Break

Authentication



Q Anarkali digitally signs a message and sends it to Salim. Verification of the signature by Salim requires **(GATE-2016) (1 Marks)**

(A) Anarkali's public key.

(B) Salim's public key.

(C) Salim's private key.

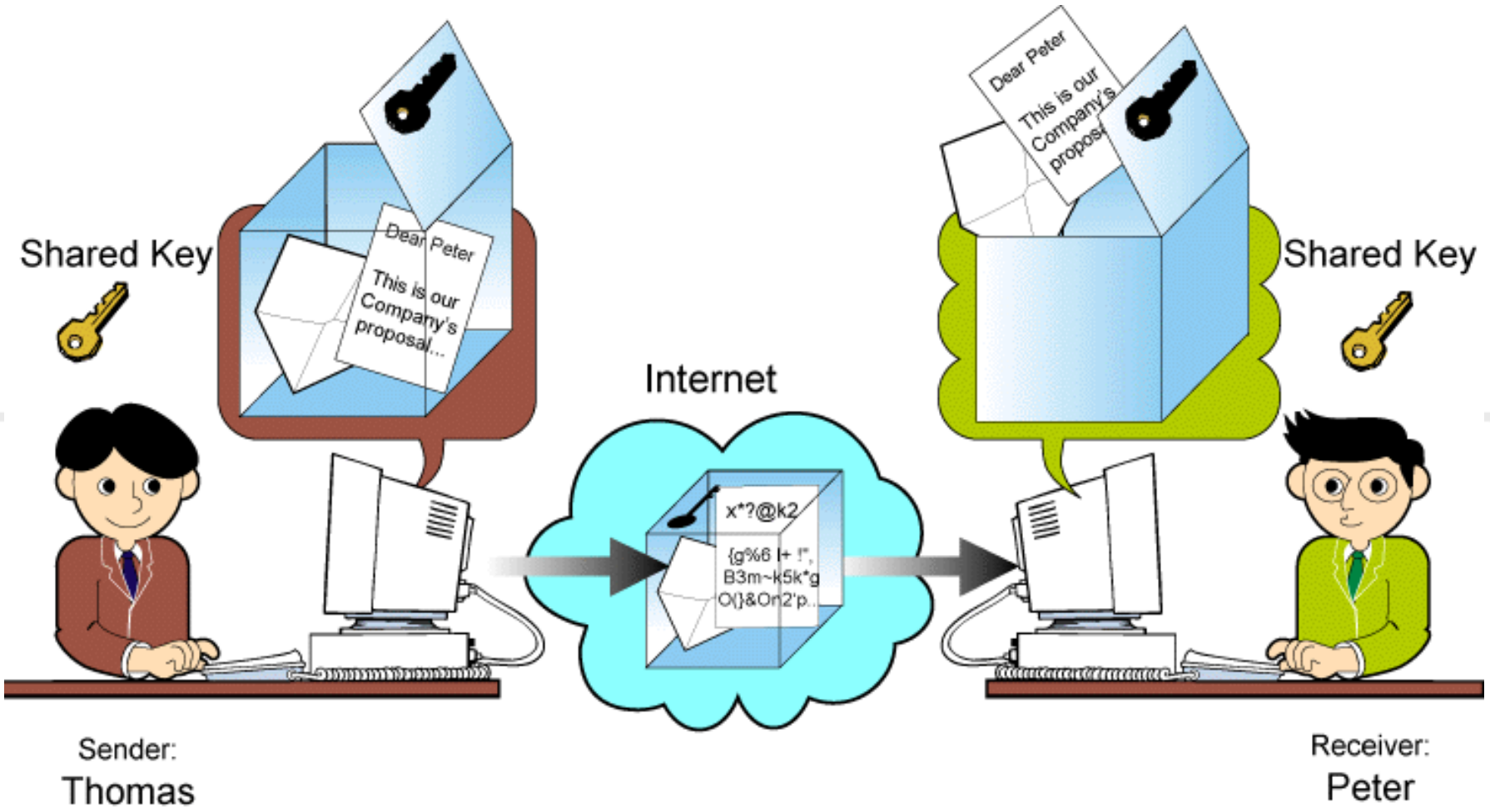
(D) Anarkali's private key.

Q Consider that B wants to send a message m that is digitally signed to A. Let the pair of private and public keys for A and B be denoted K_x^- and K_x^+ for $x = A, B$, respectively. Let $K_x(m)$ represent the operation of encrypting m with a key K_x and H(m) represent the message digest. Which one of the following indicates the CORRECT way of sending the message m along with the digital signature to A? **(GATE-2016) (2 Marks)**

(A) $\{m, K_B^+(H(m))\}$ (B) $\{m, K_B^-(H(m))\}$ (C) $\{m, K_A^-(H(m))\}$ (D) $\{m, K_A^+(m)\}$

Break

Authentication Confidentiality



Q Using public key cryptography, X adds a digital signature σ to message M, encrypts < M, σ >, and sends it to Y, where it is decrypted. Which one of the following sequences of keys is used for the operations? **(GATE-2013) (1 Marks)**

(A) Encryption: X's private key followed by Y's private key;
Decryption: X's public key followed by Y's public key

(B) Encryption: X's private key followed by Y's public key;
Decryption: X's public key followed by Y's private key

(C) Encryption: X's public key followed by Y's private key;
Decryption: Y's public key followed by X's private key

(D) Encryption: X's private key followed by Y's public key;
Decryption: Y's private key followed by X's public key

Q The total number of keys required for a set of n individuals to be able to communicate with each other using secret key and public key crypto-systems, respectively are: **(GATE-2008) (2 Marks)**

(A) n(n-1) and 2n

(B) 2n and ((n(n – 1))/2)

(C) ((n(n – 1))/2) and 2n

(D) ((n(n – 1))/2) and n

Break

RSA Algorithm

Bob chooses two large numbers, p and q, and calculates $n = p \times q$ and $\phi = (p - 1) \times (q - 1)$. Bob then selects e and d such that $(e \times d) \bmod \phi = 1$. Bob advertises e and n to the community as the public key; Bob keeps d as the private key. Anyone, including Alice, can encrypt a message and send the ciphertext to Bob, using $C = (P^e) \bmod n$; only Bob can decrypt the message, using $P = (C^d) \bmod n$. An intruder such as Eve cannot decrypt the message if p and q are very large numbers (she does not know d).

For the sake of demonstration, let Bob choose 7 and 11 as p and q and calculate $n = 7 \times 11 = 77$. The value of $\phi(n) = (7 - 1)(11 - 1)$, or 60. If he chooses e to be 13, then d is 37. Note that $e \times d \bmod 60 = 1$. Now imagine that Alice wants to send the plaintext 5 to Bob. She uses the public exponent 13 to encrypt 5. This system is not safe because p and q are small.

Plaintext: 5

$C = 5^{13} = 26 \bmod 77$

Ciphertext: 26

Ciphertext: 26

$P = 26^{37} = 5 \bmod 77$

Plaintext: 5

Here is a more realistic example calculated using a computer program in Java. We choose a 512-bit p and q, calculate n and $\phi(n)$. We then choose e and calculate d. Finally, we show the results of encryption and decryption. The integer p is a 159-digit number.

$p =$ 961303453135835045741915812806154279093098455949962158225831508796479404550564706384912571601803475031209866660649242019180878066742109606335421992666120 9

The integer q is a 160-digit number.

$q =$ 120601919572314469182767942044508960015559250546370339360617983217314821484837646592153894532091752252732268301071206956046025138871455249690003596600456 17

The modulus $n = p \times q$. It has 309 digits.

$n =$ 115935041739676149688925098646158875237714573754541447754855261376147885408326350817276878815968325168468849300625485764111250162414552339182927162507656772727460097082714127730434960500556347274566628060099924037102991424472292215772798531727033839381334692684137327622000966676671831831088373420823444370953

$\phi(n) = (p - 1)(q - 1)$ has 309 digits.

Bob chooses $e = 35535$ (the ideal is 65537). He then finds d.

$\phi(n) =$	11593504173967614968892509864615887523771457375454144775485526137614788540832635081727687881596832516846884930062548576411125016241455233918292716250765675105423360849291675203448262798811755478765701392344405716989581728196098226361075467211864612171359107358640614008885170265377277264467341066243857664128
$e =$	35535
$d =$	58008302860037763936093661289677917594669062089650962180422866111380593852822358731706286910030021710859044338402170729869087600611530620252495988444804756824096624708148581713046324064407770483313401085094738529564507193677406119732655742423721761767462077637164207600337085333288532144708859551366702948 31

Alice wants to send the message "THIS IS A TEST", which can be changed to a numeric value using the 00–26 encoding scheme (26 is the *space* character).

The ciphertext calculated by Alice is $C = P^e$, which is shown below.

P =	19070818260818260026190418 19
C =	475309123646226827206365550610545180942371796070491716523923924305445296061319932856661784341835911415119741125200568297979457173603610127821884789274156609048002350719071527718591497518846588863210114835410336165789846796838676373376577746562507928052114814184404814184430812773059004692874248559166462108656

Bob can recover the plaintext from the ciphertext using $P = C^d$, which is shown below.

P =	19070818260818260026190418 19

The recovered plaintext is "THIS IS A TEST" after decoding.

Q In a RSA cryptosystem a particular A uses two prime numbers p = 13 and q =17 to generate her public and private keys. If the public key of A is 35. Then the private key of A is _____.

(GATE-2017) (2 Marks)

Q In the RSA public key cryptosystem, the private and public keys are (e, n) and (d, n) respectively, where n = p*q and p and q are large primes. Besides, n is public and p and q are private. Let M be an integer such that 0 < M < n and f(n) = (p- 1)(q-1). Now consider the following equations.

I. $M' = M^e \bmod n$, $M = (M')^d \bmod n$

II. $ed \equiv 1 \bmod n$

III. $ed \equiv 1 \bmod f(n)$

IV. $M' = M^e \bmod f(n)$, $M = (M')^d \bmod f(n)$

Which of the above equations correctly represent RSA cryptosystem? **(GATE-2009) (2 Marks)**

(A) I and II **(B)** I and III **(C)** II and IV **(D)** III and IV

Q A sender is employing public key cryptography to send a secret message to a receiver. Which one of the following statements is TRUE? **(GATE-2004) (1 Marks)**

(A) Sender encrypts using receiver's public key

(B) Sender encrypts using his own public key

(C) Receiver decrypts using sender's public key

(D) Receiver decrypts using his own public key

Break

Fermat little theorem

Q The minimum positive integer p such that 3^p modulo 17 = 1 is **(GATE-2007) (1 Marks)**

(A) 5 **(B)** 8 **(C)** 12 **(D)** 16

Break

Diffie Hellman

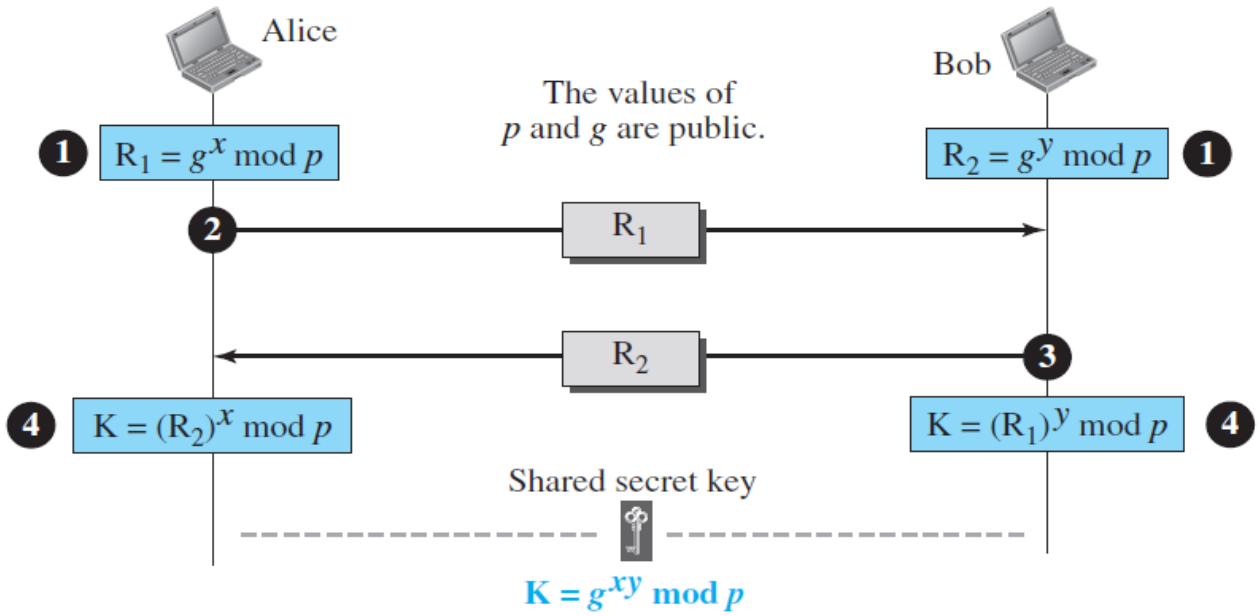
In the **Diffie-Hellman protocol** two parties create a symmetric session key without the need of a KDC. Before establishing a symmetric key, the two parties need to choose two numbers p and g. These two numbers have some properties discussed in number theory, but that discussion is beyond the scope of this book. These two numbers do not need to be confidential. They can be sent through the Internet; they can be public.

The steps are as follows:

1. Alice chooses a large random number x such that $0 \le x \le p - 1$ and calculates $R_1 = g^x \bmod p$. Bob chooses another large random number y such that $0 \le y \le p - 1$ and calculates $R_2 = g^y \bmod p$.
2. Alice sends R_1 to Bob. Note that Alice does not send the value of x; she sends only R_1.
3. Bob sends R_2 to Alice. Again, note that Bob does not send the value of y, he sends only R_2.
4. Alice calculates $K = (R_2)^x \bmod p$. Bob also calculates $K = (R_1)^y \bmod p$.

K is the symmetric key for the session.

$$K = (g^x \bmod p)^y \bmod p = (g^y \bmod p)^x \bmod p = g^{xy} \bmod p$$



Bob has calculated $K = (R_1)^y \bmod p = (g^x \bmod p)^y \bmod p = g^{xy} \bmod p$. Alice has calculated $K = (R_2)^x \bmod p = (g^y \bmod p)^x \bmod = g^{xy} \bmod p$. Both have reached the same value without Bob knowing the value of x and without Alice knowing the value of y.

The symmetric (shared) key in the Diffie-Hellman method is $K = g^{xy} \bmod p$.

Let us give a trivial example to make the procedure clear. Our example uses small numbers, but note that in a real situation, the numbers are very large. Assume that $g = 7$ and $p = 23$. The steps are as follows:

1. Alice chooses $x = 3$ and calculates $R_1 = 7^3 \bmod 23 = 21$. Bob chooses $y = 6$ and calculates $R_2 = 7^6 \bmod 23 = 4$.
2. Alice sends the number 21 to Bob.
3. Bob sends the number 4 to Alice.
4. Alice calculates the symmetric key $K = 4^3 \bmod 23 = 18$. Bob calculates the symmetric key $K = 21^6 \bmod 23 = 18$.
   The value of K is the same for both Alice and Bob; $g^{xy} \bmod p = 7^{18} \bmod 23 = 18$.

Q Suppose that two parties A and B wish to setup a common secret key (D-H key) between themselves using the Diffie-Hellman key exchange technique. They agree on 7 as the modulus and 3 as the primitive root. Party A chooses 2 and party B chooses 5 as their respective secrets. Their D-H key is **(GATE-2005) (2 Marks)**

(A) 3 **(B)** 4 **(C)** 5 **(D)** 6

Break

Q Which of the following are used to generate a message digest by the network security protocols? **(GATE-2014) (1 Marks)**

(P) RSA **(Q)** SHA-1 **(R)** DES **(S)** MD5

(A) P and R only **(B)** Q and R only **(C)** Q and S only **(D)** R and S only

Q A layer-4 firewall (a device that can look at all protocol headers up to the transport layer) CANNOT **(Gate-2011) (1 Marks)**

(A) block HTTP traffic during 9:00PM and 5:00AM

(B) block all ICMP traffic

(C) stop incoming traffic from a specific IP address but allow outgoing traffic to same IP

(D) block TCP traffic from a specific user on a specific IP address on multi-user system during 9:00PM and 5:00AM

Q An IP machine Q has a path to another IP machine H via three IP routers R_1, R_2, and R_3.

$Q—R_1—R_2—R_3—H$

H acts as an HTTP server, and Q connects to H via HTTP and downloads a file. Session layer encryption is used, with DES as the shared key encryption protocol. Consider the following four pieces of information:

$[I_1]$ The URL of the file downloaded by Q
$[I_2]$ The TCP port numbers at Q and H
$[I_3]$ The IP addresses of Q and H
$[I_4]$ The link layer addresses of Q and H

Which of I1, I2, I3, and I4 can an intruder learn through sniffing at R2 alone? **(GATE-2014) (2 Marks)**

(A) Only I1 and I2 **(B)** Only I1 **(C)** Only I2 and I3 **(D)** Only I3 and I4