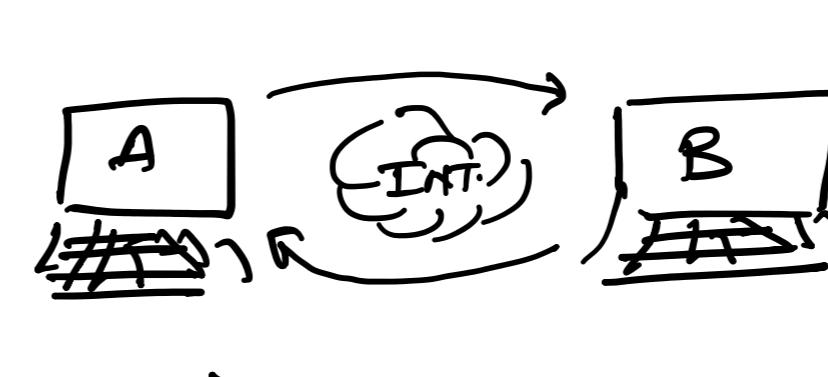


3.5

ZAFAR      Plaintext  
A B G B S      Cipher text



Data exchange over Internet.

Plain text → Cipher text  
Encryption (Public key)

Cipher text → Plain text  
Decryption (Private key)

key terms:

**Plaintext:** The original text, document or message before it is put through an encryption algorithm.

**Ciphertext:** The product when plaintext is put through an encryption algo.

**Encryption:** It is encoding of plaintext into ciphertext.

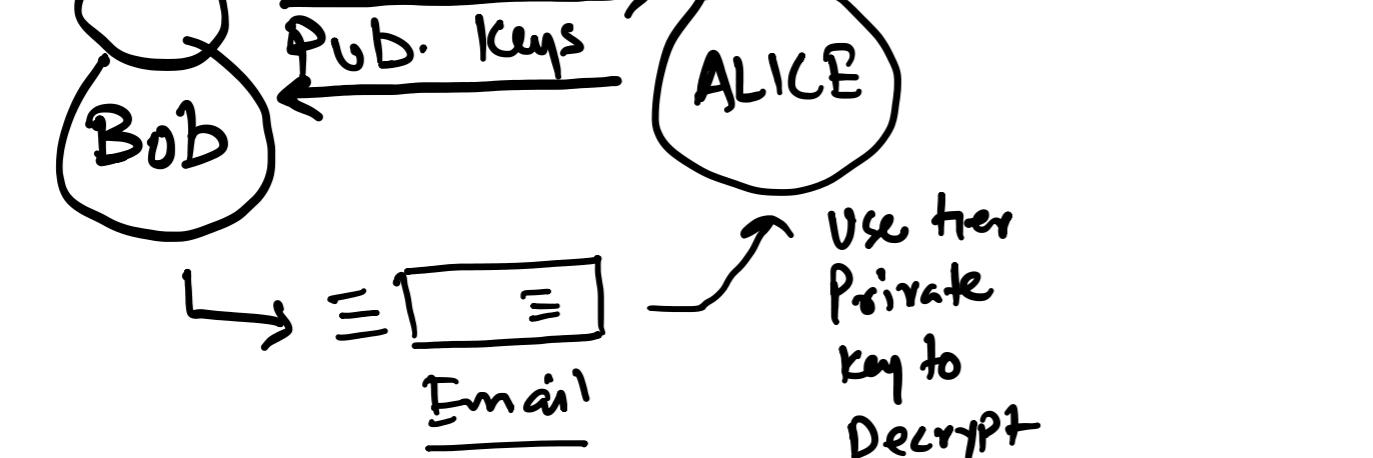
There are two types:

**Symmetric encryption:** It is encryption that uses same secret key to encrypt & decrypt.

**Asymmetric encryption:** It uses public keys and private keys.

**Public key:** Encryption/Decryption key known to all users.

**Private key:** Encryption/Decryption key known to a single user/computer that is owner.



Certificates

Asymmetric  
SSL (TLS)

Secured Socket Layer Security

Transport Layer Security

Public key      Private key

Exchange Pub. keys

Use their Private key to Decrypt data.

Email

Encrypt using Alice's Public key

Bob

Alice



1. Proper Communication starts b/w your computer & server only using session key.

1. Accessed gmail server as www.gmail.com.

2. Certificate is downloaded over

your computer, which contains gmail's public key.

3. Username, password &

session key will be encrypted using server's public key & sent to server.

4. Server will use its

private key to decrypt msg. and checks un & pw.

Further, server will use

its session key & send a test msg. called welcome msg.

5. Proper communication starts b/w your computer & server only using session key.

6. Session key will be used to decrypt msg. and check un & pw.

7. Server will use its

private key to decrypt msg. and checks un & pw.

8. Further, server will use

its session key & send a test msg. called welcome msg.

9. Proper communication starts b/w your computer & server only using session key.

10. Session key will be used to decrypt msg. and check un & pw.

11. Further, server will use

its session key & send a test msg. called welcome msg.

12. Proper communication starts b/w your computer & server only using session key.

13. Session key will be used to decrypt msg. and check un & pw.

14. Further, server will use

its session key & send a test msg. called welcome msg.

15. Proper communication starts b/w your computer & server only using session key.

16. Session key will be used to decrypt msg. and check un & pw.

17. Further, server will use

its session key & send a test msg. called welcome msg.

18. Proper communication starts b/w your computer & server only using session key.

19. Session key will be used to decrypt msg. and check un & pw.

20. Further, server will use

its session key & send a test msg. called welcome msg.

21. Proper communication starts b/w your computer & server only using session key.

22. Session key will be used to decrypt msg. and check un & pw.

23. Further, server will use

its session key & send a test msg. called welcome msg.

24. Proper communication starts b/w your computer & server only using session key.

25. Session key will be used to decrypt msg. and check un & pw.

26. Further, server will use

its session key & send a test msg. called welcome msg.

27. Proper communication starts b/w your computer & server only using session key.

28. Session key will be used to decrypt msg. and check un & pw.

29. Further, server will use

its session key & send a test msg. called welcome msg.

30. Proper communication starts b/w your computer & server only using session key.

31. Session key will be used to decrypt msg. and check un & pw.

32. Further, server will use

its session key & send a test msg. called welcome msg.

33. Proper communication starts b/w your computer & server only using session key.

34. Session key will be used to decrypt msg. and check un & pw.

35. Further, server will use

its session key & send a test msg. called welcome msg.

36. Proper communication starts b/w your computer & server only using session key.

37. Session key will be used to decrypt msg. and check un & pw.

38. Further, server will use

its session key & send a test msg. called welcome msg.

39. Proper communication starts b/w your computer & server only using session key.

40. Session key will be used to decrypt msg. and check un & pw.

41. Further, server will use

its session key & send a test msg. called welcome msg.

42. Proper communication starts b/w your computer & server only using session key.

43. Session key will be used to decrypt msg. and check un & pw.

44. Further, server will use

its session key & send a test msg. called welcome msg.

45. Proper communication starts b/w your computer & server only using session key.

46. Session key will be used to decrypt msg. and check un & pw.

47. Further, server will use

its session key & send a test msg. called welcome msg.

48. Proper communication starts b/w your computer & server only using session key.

49. Session key will be used to decrypt msg. and check un & pw.

50. Further, server will use

its session key & send a test msg. called welcome msg.

51. Proper communication starts b/w your computer & server only using session key.

52. Session key will be used to decrypt msg. and check un & pw.

53. Further, server will use

its session key & send a test msg. called welcome msg.

54. Proper communication starts b/w your computer & server only using session key.

55. Session key will be used to decrypt msg. and check un & pw.

56. Further, server will use

its session key & send a test msg. called welcome msg.

57. Proper communication starts b/w your computer & server only using session key.

58. Session key will be used to decrypt msg. and check un & pw.

59. Further, server will use

its session key & send a test msg. called welcome msg.

60. Proper communication starts b/w your computer & server only using session key.

61. Session key will be used to decrypt msg. and check un & pw.

62. Further, server will use

its session key & send a test msg. called welcome msg.

63. Proper communication starts b/w your computer & server only using session key.

64. Session key will be used to decrypt msg. and check un & pw.

65. Further, server will use

its session key & send a test msg. called welcome msg.

66. Proper communication starts b/w your computer & server only using session key.

67. Session key will be used to decrypt msg. and check un & pw.

68. Further, server will use

its session key & send a test msg. called welcome msg.

69. Proper communication starts b/w your computer & server only using session key.

70. Session key will be used to decrypt msg. and check un & pw.

71. Further, server will use

its session key & send a test msg. called welcome msg.

72. Proper communication starts b/w your computer & server only using session key.

73. Session key will be used to decrypt msg. and check un & pw.

74. Further, server will use

its session key & send a test msg. called welcome msg.

75. Proper communication starts b/w your computer & server only using session key.

76. Session key will be used to decrypt msg. and check un & pw.

77. Further, server will use

its session key & send a test msg. called welcome msg.

78. Proper communication starts b/w your computer & server only using session key.

79. Session key will be used to decrypt msg. and check un & pw.

80. Further, server will use

its session key & send a test msg. called welcome msg.

81. Proper communication starts b/w your computer & server only using session key.

82. Session key will be used to decrypt msg. and check un & pw.

83. Further, server will use

its session key & send a test msg. called welcome msg.

84. Proper communication starts b/w your computer & server only using session key.

85. Session key will be used to decrypt msg. and check un & pw.

86. Further, server will use

its session key & send a test msg. called welcome msg.

87. Proper communication starts b/w your computer & server only using session key.

88. Session key will be used to decrypt msg. and check un & pw.

89. Further, server will use

its session key & send a test msg. called welcome msg.

90. Proper communication starts b/w your computer & server only using session key.

91. Session key will be used to decrypt msg. and check un & pw.

92. Further, server will use

its session key & send a test msg. called welcome msg.