Graduate Certificate in AI in Banking Security

Advanced Encryption Techniques for Secure Transactions

Encryption is a crucial component of modern banking security systems, especially for secure transactions. It is the process of converting plaintext data into ciphertext, which is unreadable without the correct decryption key. Advanced Encryption Techniques refer to sophisticated methods used to secure data and communications. In this course, we will explore various encryption algorithms, protocols, and best practices to ensure the confidentiality, integrity, and authenticity of banking transactions.

Key Terms and Vocabulary:

1. **Encryption**: The process of converting plaintext data into ciphertext to secure it from unauthorized access.

2. **Decryption**: The reverse process of encryption, converting ciphertext back into plaintext using the correct decryption key.

3. **Ciphertext**: The encrypted form of data, which is unreadable without the decryption key.

4. **Plaintext**: The original, unencrypted form of data.

5. **Symmetric Encryption**: A type of encryption where the same key is used for both encryption and decryption.

6. **Asymmetric Encryption**: A type of encryption where a pair of keys (public and private) is used for encryption and decryption.

7. **Key**: A unique piece of information used in encryption and decryption processes.

8. **Encryption Algorithm**: A set of rules and procedures used to encrypt and decrypt data.

9. **RSA Algorithm**: A popular asymmetric encryption algorithm named after its inventors Rivest, Shamir, and Adleman.

10. **AES (Advanced Encryption Standard)**: A symmetric encryption algorithm widely used for securing data.

11. **Block Cipher**: An encryption algorithm that operates on fixed-length groups of bits called blocks.

12. **Stream Cipher**: An encryption algorithm that encrypts data one bit at a time.

13. **Key Length**: The size of the encryption key, usually measured in bits.

14. **Digital Signature**: A cryptographic technique used to verify the authenticity and integrity of a message.

15. **Hash Function**: A mathematical function that converts an input into a fixed-size string of bytes.

16. **SHA (Secure Hash Algorithm)**: A family of cryptographic hash functions used for data integrity.

17. **SSL/TLS (Secure Sockets Layer/Transport Layer Security)**: Protocols used to secure communication over a network.

18. **PKI (Public Key Infrastructure)**: A system for managing public-key encryption.

19. **Certificate**: A digital document used to prove the ownership of a public key.

20. **Key Exchange**: The process of securely exchanging encryption keys between parties.

21. **Digital Certificate**: A digital document that binds a public key to an individual or entity.

22. **End-to-End Encryption**: A method of secure communication where only the communicating users can read the messages.

23. **Zero-Knowledge Proof**: A cryptographic method to prove knowledge of a secret without revealing the secret itself.

24. **Homomorphic Encryption**: An encryption scheme that allows computations to be performed on encrypted data without decrypting it.

25. **Quantum Cryptography**: A cryptographic method based on quantum mechanics principles for secure communication.

26. **Challenge-Response Authentication**: A method where one party challenges the other to prove its identity.

27. **Cryptanalysis**: The study of analyzing and breaking encryption systems.

28. **Side-Channel Attack**: An attack that exploits information leaked during the encryption process.

29. **Key Management**: The process of generating, storing, distributing, and revoking encryption keys securely.

30. **Key Escrow**: A process where a trusted third party holds a copy of encryption keys for recovery purposes.

31. **Secure Enclave**: A hardware-based security feature for storing encryption keys securely.

32. **Quantum Key Distribution (QKD)**: A method of secure key exchange using quantum mechanics principles.

33. **Multi-Factor Authentication**: A security process that requires multiple forms of verification to access an account.

34. **Biometric Authentication**: A security method that uses unique biological characteristics such as fingerprints or facial recognition for authentication.

35. **Tokenization**: The process of replacing sensitive data with unique identifiers called tokens.

36. **Data Masking**: A technique used to hide sensitive data by replacing it with fictional or random data.

37. **Data Loss Prevention (DLP)**: Technologies and strategies used to prevent the unauthorized transmission of sensitive data.

38. **Secure Communication Channel**: A secure pathway for transmitting data between two parties.

39. **Blockchain**: A distributed ledger technology that ensures the integrity and immutability of transactions.

40. **Cryptocurrency**: Digital or virtual currencies secured by cryptography.

41. **Key Pair**: A set of two keys (public and private) used in asymmetric encryption.

42. **Key Derivation Function (KDF)**: A cryptographic function used to derive encryption keys from a master key.

43. **Perfect Forward Secrecy (PFS)**: A property that ensures that compromising a single key does not compromise past or future communication.

44. **Quantum-Safe Cryptography**: Encryption algorithms designed to resist attacks from quantum computers.

45. **Post-Quantum Cryptography**: Cryptographic methods that are secure against quantum computers.

46. **Confidentiality**: Ensuring that data is only accessible to authorized parties.

47. **Integrity**: Ensuring that data is not tampered with during transmission or storage.

48. **Authentication**: Verifying the identity of users or systems.

49. **Non-Repudiation**: Ensuring that a sender cannot deny sending a message.

50. **Key Exchange Protocol**: A set of rules for securely exchanging encryption keys.

51. **Secure Element**: A tamper-resistant hardware component for storing sensitive information.

52. **Side-Channel Resistance**: A property of encryption algorithms that resist side-channel attacks.

53. **Cryptographic Agility**: The ability to switch between different encryption algorithms or key lengths.

54. **Key Rotation**: The process of regularly changing encryption keys to enhance security.

55. **Data Encryption Standard (DES)**: An outdated symmetric encryption algorithm replaced by AES.

56. **Triple DES (3DES)**: A variant of DES that applies the DES algorithm three times for enhanced security.

57. **Message Authentication Code (MAC)**: A code used to authenticate the integrity and authenticity of a message.

58. **Elliptic Curve Cryptography (ECC)**: A type of public-key cryptography based on elliptic curves.

59. **Quantum-Secure Communication**: Communication methods that are secure against quantum attacks.

60. **Confusion**: A property of encryption algorithms that makes the relationship between plaintext and ciphertext complex.

61. **Diffusion**: A property of encryption algorithms that spreads the influence of a single plaintext bit over many ciphertext bits.

62. **Key Stretching**: A technique to increase the security of passwords by making them longer and more complex.

63. **Cryptographic Salt**: Random data added to passwords before hashing to prevent rainbow table attacks.

64. **Zero-Day Attack**: An attack exploiting a vulnerability unknown to the software vendor.

65. **Ransomware**: Malware that encrypts data and demands payment for decryption.

66. **Side-Channel Leakage**: Information leaked during the encryption process that can be exploited by attackers.

67. **Random Number Generator (RNG)**: A tool used to generate random numbers for encryption algorithms.

68. **Quantum Resistant Cryptography**: Encryption algorithms designed to resist attacks from quantum

computers.

69. **Certificate Authority (CA)**: An entity that issues digital certificates.

70. **Public Key**: A key used for encryption in asymmetric cryptography.

71. **Private Key**: A key used for decryption in asymmetric cryptography.

72. **Hash Collision**: When two different inputs produce the same hash output.

73. **Birthday Attack**: A type of cryptographic attack that exploits the birthday paradox to find collisions in hash functions.

74. **Cryptographic Key Agility**: The ability to change encryption keys or algorithms easily.

75. **Streamlining**: The process of optimizing encryption algorithms for better performance.

76. **FIPS (Federal Information Processing Standards)**: Standards for cryptographic algorithms and security requirements.

77. **Cryptographic Module**: Software or hardware that performs cryptographic functions.

78. **Hardware Security Module (HSM)**: A dedicated hardware device for storing encryption keys securely.

79. **Side-Channel Cryptanalysis**: Attacking encryption algorithms by analyzing information leaked during the encryption process.

80. **Entropy**: A measure of randomness used in encryption algorithms.

81. **Nonce**: A number used only once in cryptographic protocols to prevent replay attacks.

82. **Quantum Supremacy**: The point at which a quantum computer can perform a task that is infeasible for classical computers.

83. **Cryptocurrency Wallet**: Software or hardware for storing and managing cryptocurrencies.

84. **Blockchain Consensus Algorithm**: A method for achieving agreement on a single data value among distributed nodes.

85. **Elliptic Curve Digital Signature Algorithm (ECDSA)**: A digital signature scheme based on elliptic curve cryptography.

86. **Secure Multi-Party Computation (SMPC)**: A cryptographic technique for computing a function over multiple inputs without revealing the inputs.

87. **Post-Quantum Cryptography Competition**: A competition to select new cryptographic algorithms

resistant to quantum attacks.

88. **Key Exchange Algorithm**: A cryptographic protocol for securely exchanging encryption keys.

89. **Secure Boot**: A process to ensure that only trusted software is executed during system startup.

90. **Quantum-Safe Key Exchange**: A method for securely exchanging encryption keys resistant to quantum attacks.

91. **Side-Channel Countermeasure**: Techniques to mitigate side-channel attacks on encryption algorithms.

92. **Cryptographic Primitive**: A basic building block of cryptographic algorithms.

93. **Cryptographic Agility Protocol**: A protocol that supports multiple encryption algorithms for flexibility and security.

94. **Quantum Key Distribution Protocol**: A protocol for secure key exchange based on quantum mechanics principles.

95. **Cryptographic Key Agreement Protocol**: A protocol for two parties to agree on a shared encryption key.

96. **Secure Communication Protocol**: A set of rules for secure communication between parties.

97. **Blockchain Consensus Mechanism**: A method for achieving agreement on the state of a blockchain network.

98. **Cryptocurrency Mining**: The process of validating transactions and adding them to the blockchain.

99. **Zero-Knowledge Encryption**: A cryptographic technique where one party can prove knowledge of a secret without revealing the secret itself.

100. **Quantum-Secure Authentication**: Authentication methods resistant to quantum attacks.

In conclusion, mastering these key terms and vocabulary related to Advanced Encryption Techniques is essential for understanding and implementing secure transactions in banking systems. By applying these concepts effectively, banks can enhance the security of their transactions and protect customer data from unauthorized access and malicious attacks.