Transition to Post-Quantum Cryptography Standards (NIST)

- **Cryptographic Standards**
  - Digital Signature Algorithms
    - NIST-Approved Digital Signature Algorithms
      - Historical Algorithms (Vulnerable to Quantum Attacks)
        - FIPS 186 specifies:
          - Elliptic Curve Digital Signature Algorithm (ECDSA)
          - RSA Algorithm
            - Specified in RFC 8017 and PKCS #1 (version 1.5 and higher)
          - Edwards-Curve Digital Signature Algorithm (EdDSA)
            - Specified in RFC 8032
        - SP 800-186 specifies:
          - Elliptic Curves used with ECDSA
          - Elliptic Curve Cryptography (ECC)-Based Key Establishment Schemes
            - Defined in SP 800-56A
        - Vulnerability
          - All above algorithms are susceptible to Shor's Algorithm on a quantum computer.
            - Shor's Algorithm: An algorithm capable of breaking RSA, ECDSA, and EdDSA when implemented on a quantum computer.
      - Quantum-Resistant Digital Signature Schemes
        - FIPS 204: Module-Lattice-Based Digital Signature Algorithm (ML-DSA)
          - Derived From
            - CRYSTALS-Dilithium submission
          - Features
            - Quantum-resistant lattice-based algorithm
        - FIPS 205: Stateless Hash-Based Digital Signature Algorithm (SLH-DSA)
          - Derived From
            - SPHINCS+ submission
          - Features
            - Stateless hash-based algorithm
            - Quantum-resistant
        - SP 800-208: Stateful Hash-Based Signature (HBS) Schemes
          - Algorithms
            - Leighton-Micali Signature (LMS) System
            - eXtended Merkle Signature Scheme (XMSS)
          - Multi-Tree Variants
            - Hierarchical Signature System (HSS)
            - Multi-Tree XMSS (XMSSMT)
          - Features
            - Quantum Resistance
              - Resistant to quantum computer attacks
            - Private Key Structure
              - Composed of a large set of One-Time Signature (OTS) Private Keys
            - Security Reliance
              - Ensures no OTS key is used more than once
            - Limitations
              - Requires maintaining state (tracking OTS key usage)
              - Not intended for general use due to statefulness
      - Future NIST Plans
        - Development of New Standards
          - FIPS Derived from FALCON Algorithm
            - Purpose: To provide an additional quantum-resistant digital signature alternative
            - Status: NIST intends to develop this standard
        - Evaluation of Additional Algorithms
          - Additional Digital Signature Schemes for Standardization
            - Process: NIST Post-Quantum Cryptography Standardization Process
            - Objective: Assess other proposed quantum-resistant digital signature algorithms for potential standardization
  - Key Establishment
    - Current NIST-Approved Key-Establishment Schemes
      - SP 800-56A: Pair-Wise Key-Establishment Using Discrete Logarithm-Based Cryptography
        - Focus
          - Based on the Discrete Logarithm Problem over:
            - Finite fields
            - Elliptic curves
        - Key Establishment Schemes
          - Diffie-Hellman (DH) Variants
          - Menezes-Qu-Vanstone (MQV) Variants
      - SP 800-56B: Pair-Wise Key-Establishment Using Integer Factorization Cryptography
        - Focus
          - Based on the RSA Public Key Cryptosystem
        - Includes Methods for
          - Key Agreement
          - Key Transport
    - Quantum-Resistant Key Establishment
      - FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)
        - Derived From
          - CRYSTALS-KYBER Submission
        - Purpose
          - Establish shared secret keys over a public channel.
        - Type
          - Key Encapsulation Mechanism (KEM): A specific type of key-establishment scheme.
      - Future Developments
        - NIST PQC Standardization Process
          - Fourth Round: Evaluating additional KEM algorithms.
          - Objective: Select one or more alternatives to ML-KEM
  - Symmetric Cryptography
    - Classes of Symmetric-Key Algorithms
      - Block Cipher Algorithms
        - Example: AES (Advanced Encryption Standard)
      - Hash-Based Constructions
        - Example: Keyed-Hash Message Authentication Code (HMAC) based on a hash function.
    - Applications of Symmetric-Key Algorithms
      - Encryption
        - Using Block Cipher Modes of Operation
          - Modes specify how block ciphers process plaintext into ciphertext.
      - Data Authentication
        - Using Block Cipher Modes of Operation
          - Ensures the integrity and authenticity of data.
        - Using Key-Hash Constructions
          - HMAC or similar mechanisms.
      - Key Management
        - Key Derivation
          - Generating cryptographic keys from shared secrets.
        - Key Wrapping
          - Securing cryptographic keys for storage or transport.
      - Randomness
        - Random Bit Generation
          - Generating cryptographically secure random numbers.
    - Security Against Quantum Attacks
      - Quantum Resistance
        - Existing Standards
          - Symmetric cryptography standards (e.g., AES) are less vulnerable to quantum attacks compared to asymmetric algorithms.
        - NIST Expectation
          - Transition to Post-Quantum Cryptography (PQC) will not require significant changes to symmetric cryptography standards.
- **Cryptographic Technologies and Components**
  - Network Protocol and Security Technology Standards
    - Cryptographic Dependencies
      - Current State
        - Rely on classical cryptographic algorithms.
        - Vulnerable to quantum attacks.
      - Need for Updates
        - Objective:
          - Incorporate Post-Quantum Cryptography (PQC) algorithms.
        - Importance:
          - Maintain data confidentiality and integrity in a quantum-enabled world.
    - Updating Protocols for PQC
      - Revision Requirements
        - Key Exchange Mechanisms
          - Introduce quantum-resistant key exchange methods.
        - Authentication Methods
          - Update to quantum-resistant authentication algorithms.
      - Nature of Changes
        - Simple Update
          - Assign an identifier for new algorithms.
        - Significant Revisions
          - Accommodate
            - Larger Key Sizes: PQC algorithms often require larger keys.
            - Different Interfaces: New algorithms may have unique operational requirements.
    - Key Challenges in Protocol Updates
      - Larger Key Sizes
        - PQC algorithms typically use larger key sizes than classical algorithms.
        - Impacts
          - Bandwidth requirements.
          - Performance.
      - Algorithm Interface Differences
        - New algorithms may
          - Operate differently.
          - Require structural changes to protocols.
      - Backward Compatibility
        - Ensure updates do not disrupt existing systems during transition.
  - Software Cryptographic Libraries
    - Transition to Post-Quantum Cryptography (PQC)
      - Need for Incorporation
        - Standardization:
          - Incorporate PQC algorithms standardized by bodies like NIST.
        - Purpose
          - Ensure access to quantum-resistant cryptographic functions.
          - Simplify implementation for developers by avoiding the need to implement complex algorithms themselves.
      - Benefits of Updating
        - Security Enhancement
          - Protect against future quantum computer attacks.
        - Developer Convenience
          - Provide ready-to-use quantum-resistant functions.
        - Performance Optimization
          - Improve the efficiency of cryptographic operations.
    - Steps Involved in Transition
      - Adding New Algorithms
        - Integration
          - Incorporate newly standardized PQC algorithms into existing libraries.
        - Support
          - Ensure compatibility with existing cryptographic protocols and applications.
      - Optimizing Implementations for Performance
        - Efficiency
          - Enhance the performance of PQC algorithms to meet practical application needs.
        - Resource Management
          - Optimize memory and processing requirements for seamless operation.
      - Ensuring Security Against Side-Channel Attacks
        - Mitigation Techniques
          - Implement strategies to protect against side-channel attacks.
        - Secure Coding Practices
          - Follow best practices to minimize vulnerabilities in PQC implementations.
    - Challenges in Updating Libraries
      - Performance Optimization
        - Complexity of PQC Algorithms
          - Larger key sizes and more complex operations can impact performance.
        - Balancing Security and Efficiency
          - Ensuring that optimizations do not compromise security.
      - Security Assurance
        - Side-Channel Attack Resistance
          - Developing implementations that are robust against various attack vectors.
        - Continuous Monitoring
          - Regularly updating and patching libraries to address emerging threats.
      - Compatibility and Integration
        - Backward Compatibility
          - Ensuring new PQC algorithms integrate smoothly with existing systems.
        - Interoperability
          - Facilitating communication between updated libraries and other cryptographic components.
  - Cryptographic Hardware
    - Applications of Cryptographic Hardware
      - Server Infrastructure Security
        - Purpose: Secure cryptographic operations for server environments.
        - Examples
          - Data encryption.
          - Secure communications.
      - Personal Device Security
        - Purpose: Protect sensitive cryptographic keys on user devices.
        - Examples
          - Secure boot processes.
          - Hardware-based authentication.
    - Transition to Post-Quantum Cryptography (PQC)
      - Need for Upgrades
        - PQC Requirements
          - Larger key sizes.
          - Different computational demands.
      - Upgrade Scope
        - Firmware Updates
          - Modify existing firmware to support new algorithms.
        - Hardware Redesigns
          - Adapt hardware for efficient PQC operations.
  - PKI and Other Infrastructure Components
    - Transition to Post-Quantum Cryptography (PQC)
      - Update Requirements for PKI
        - Certificate Management
          - Issue, distribute, and manage certificates using PQC algorithms.
        - Digital Signatures
          - Sign certificates and revocation status information using quantum-resistant cryptographic methods.
      - Modifications in Processes
        - Certificate Issuance
          - Support new cryptographic algorithms in the issuance process.
        - Validation and Revocation
          - Update mechanisms to accommodate PQC-based certificates and signatures.
  - IT Applications and Services
    - Transition to Post-Quantum Cryptography (PQC)
      - Need for Updates
        - Support PQC algorithms for:
          - Digital Signatures
          - Encryption
          - Key Exchange
      - Changes Required
        - Cryptographic Implementations:
          - Replace or upgrade classical algorithms with quantum-resistant alternatives.
        - Key Sizes and Algorithm Performance:
          - Adjust applications to handle larger key sizes and computational overhead.
        - Protocol and Library Compatibility:
          - Ensure seamless integration with updated cryptographic libraries and standards.
    - Development and Testing Requirements
      - Code Refactoring
        - Modify existing application code to incorporate PQC algorithms.
      - Testing
        - Focus Areas
          - Functional Testing: Ensure the application behaves as expected.
          - Performance Testing: Measure the impact of PQC algorithms on system efficiency.
          - Security Testing: Validate resistance against quantum and classical attacks.
      - User Interface (UI) Redesign
        - User Interface (UI) Redesign
          - Purpose
            - Accommodate changes related to larger key sizes or additional cryptographic options.
          - Potential Changes
            - Inform users about new cryptographic standards and security updates.
- **Migration Considerations**
  - Use Cases
    - Code Signing
      - Quantum-resistant signatures for long-lifespan devices.
    - User and Machine Authentication
      - Upgrade systems to support PQC.
      - Secure long-term-sensitive systems.
    - Network Security Protocols
      - Migrate key-establishment schemes first (addresses "harvest now, decrypt later").
      - Transition authentication algorithms later.
    - Email and Document Signing and Encryption
      - Address integrity and confidentiality.
      - Update S/MIME for PQC encryption and signing.
  - PQC-Classical Hybrid Protocols
    - Hybrid Key-Establishment Techniques
      - Mechanism
        - Combine multiple key-establishment schemes into a composite system.
      - Standards
        - SP 800-56C: Composite Key-Establishment Techniques.
        - FIPS 203: Use shared secrets as inputs for hybrid methods.
      - Future Guidance
        - SP 800-227: Recommendations for Key Encapsulation Mechanisms.
    - Hybrid Digital Signature Techniques
      - Mechanism
        - Use dual signatures (multiple signatures on the same message).
      - Applications
        - Signing data and certificates within PKI.
      - NIST Role
        - Provide guidance for integrating hybrid modes into FIPS 140 validation.
- **Towards a PQC Standards Transition Timeline**
  - NIST Cryptographic Algorithm Standards and Guidelines
    - Transition Framework
      - SP 800-131A: Defines algorithm approval statuses.
        - Acceptable: Fully approved.
        - Deprecated: Can be used with caution due to security risks.
        - Disallowed: No longer allowed.
        - Legacy Use: Permitted only for processing already protected data.
      - Transition schedules guided by security strength and application specific needs.
    - Cryptographic Algorithm Standards
      - Post-Quantum Security Categories
      - Digital Signatures
        - Post-Quantum Algorithms
      - Key Establishment
        - Post-Quantum Algorithms
      - Symmetric Cryptography
        - Post-Quantum Algorithms
  - Migration Planning
    - Timelines
      - 2035: Target for full migration to PQC in Federal systems.
      - 2030: Deprecation of classical algorithms with 112-bit security.
    - Application-Specific Standards
      - Tailored guidelines based on:
        - System risks.
        - Sensitivity of data.
        - Available PQC support.
    - Hybrid Solutions
      - Techniques
        - Hybrid Key Establishment:
          - SP 800-56C: Composite key-establishment methods.
        - Hybrid Digital Signatures:
          - Dual-signature techniques for redundancy.
      - Use Cases
        - Interim solution for compatibility and risk mitigation.
        - Expected to phase out in favor of pure PQC systems.
  - Application-Specific Standards and Guidelines