Национальный Институт Стандартов и Технологий США

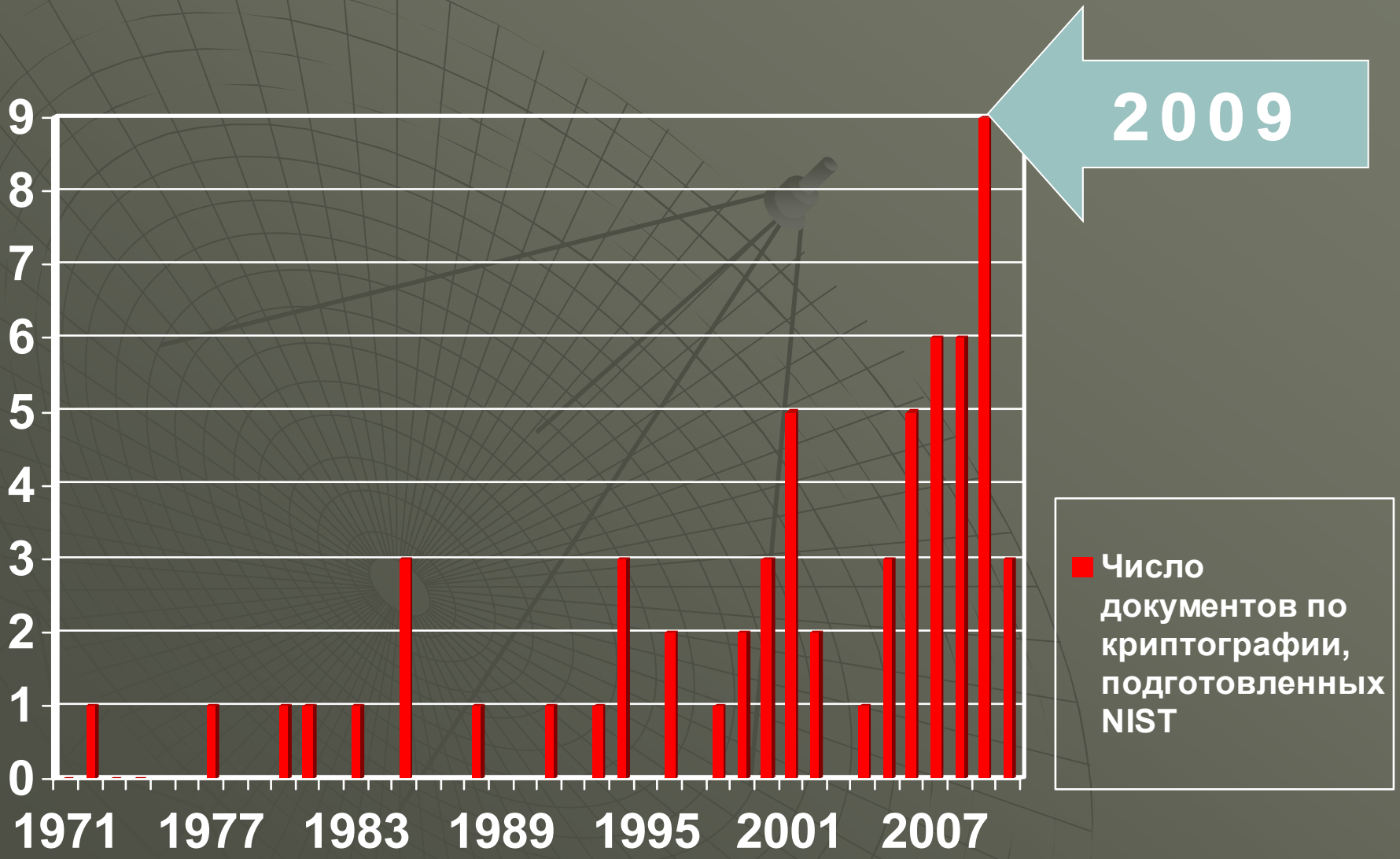
Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce.

NIST National Institute of Standards and Technology
Information Technology Laboratory

NIST's mission:
To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Development and use of standards

Публикации NIST по криптографии



2006 г.

1. **FIPS 200** *Minimum Security Requirements for Federal Information and Information Systems*
2. **SP 800-53 Rev. 1** *Recommended Security Controls for Federal Information Systems*
3. **SP 800-63 Version 1.0.2** *Electronic Authentication Guideline*
4. **SP 800-89** *Recommendation for Obtaining Assurances for Digital Signature Applications*
5. **ITL May 2006** *An Update On Cryptographic Standards, Guidelines, And Testing Requirements - ITL Security Bulletin*

2007 г.

1. **SP 800-38 D** *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*
2. **SP 800-53 Rev. 2** *Recommended Security Controls for Federal Information Systems*
3. **SP 800-56 A** *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*
4. **SP 800-57** *Recommendation for Key Management*
5. **SP 800-90** *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*
6. **SP 800-111** *Guide to Storage Encryption Technologies for End User Devices*

2008 г.

1. **FIPS 180-3** *Secure Hash Standard (SHS)*
2. **FIPS 198-1** *The Keyed-Hash Message Authentication Code (HMAC)*
3. **SP 800-22 Rev. 1** *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*
4. **SP 800-63 Rev. 1** (DRAFT) *Electronic Authentication Guideline*
5. **SP 800-67 1.1** *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*
6. **NIST IR 7539** *Symmetric Key Injection onto Smart Cards*

2009 г.

1. **FIPS 140-3** *Security Requirements for Cryptographic Modules (Revised Draft)*
2. **FIPS 186-3** *Digital Signature Standard (DSS)*
3. **SP 800-53** Rev. 3 *Recommended Security Controls for Federal Information Systems and Organizations*
4. **SP 800-56 B** *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*
5. **SP 800-102** *Recommendation for Digital Signature Timeliness*
6. **SP 800-106** *Randomized Hashing for Digital Signatures*
7. **SP 800-107** *Recommendation for Applications Using Approved Hash Algorithms*
8. **SP 800-108** *Recommendation for Key Derivation Using Pseudorandom Functions*
9. **SP 800-118** (DRAFT) *Guide to Enterprise Password Management*

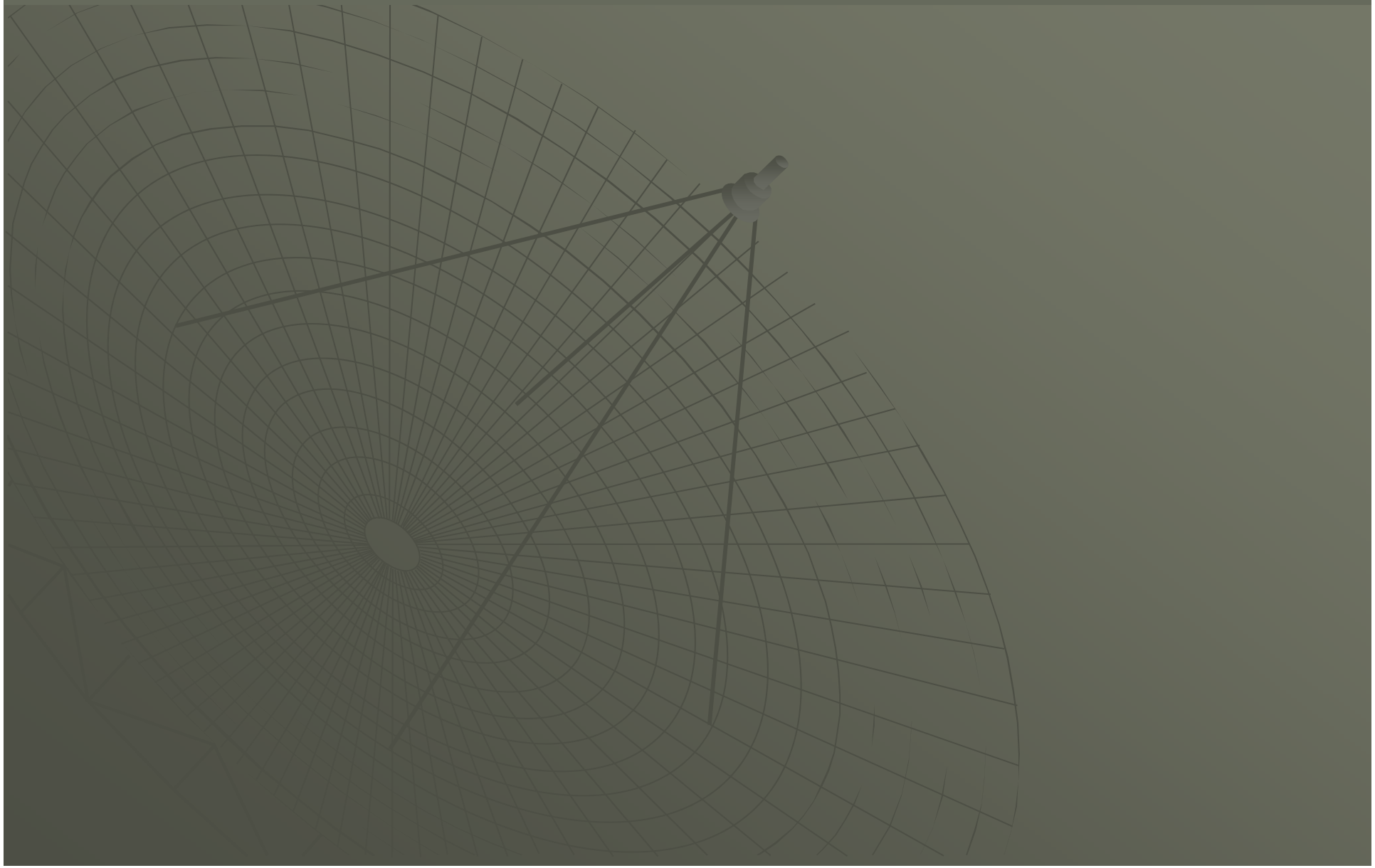
2010 г.

1. **SP 800-38 E** ***Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices***
2. **SP 800-78 -2** ***Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV)***
3. **SP 800-131** **(DRAFT)** ***Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes***

Публикации NIST по криптографии

- Block Ciphers
- Block Cipher Modes
- Digital Signatures
- Entity Authentication
- Message Authentication
- Secure Hashing
- Key Management
- Key Derivation Functions
- Password Usage and Generation
- Random Number Generation
- Implementation Guideline

Block Ciphers



Block Ciphers

Approved encryption algorithms:
AES, Triple DES (TDES, TDEA), Skipjack

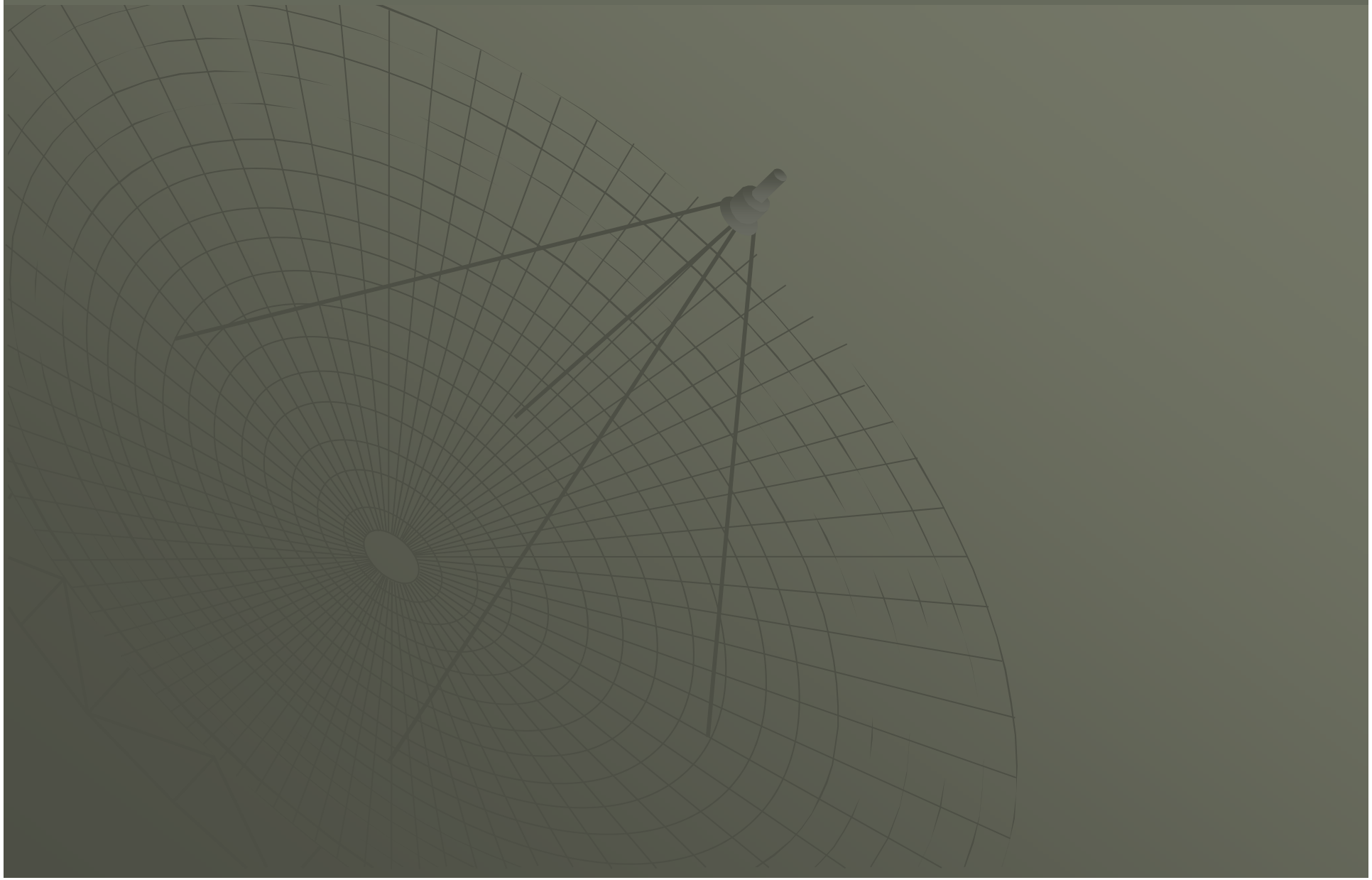
- **Advanced Encryption Standard (AES)**
- **FIPS 197**, ***Advanced Encryption Standard (AES)*** **– (Nov. 2001).**
- **CNSS Policy No. 15, Fact Sheet No. 1** ***National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information*** **- (Jun. 2003).**

Block Ciphers

- **Triple DES**
- **SP 800-67**, ***Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*** **– (May 2008).**
- **FIPS 46-3,** ***Data Encryption Standard (DES)*** **- (Oct. 1999) - has been withdrawn.**

- **Skipjack**
- **FIPS 185**, ***Escrowed Encryption Standard (EES)*** **- (Feb. 1994).**

Block Cipher Modes



Block Cipher Modes

- **Five Confidentiality Modes (updated versions of the ECB, CBC, CFB, OFB and the CTR mode)**
- **SP 800-38 A *Recommendation for Block Cipher Modes of Operation - Methods and Techniques* – (Dec. 2001).**
- **FIPS 81, *DES Modes of Operation* - (Dec. 1980) - has been withdrawn.**

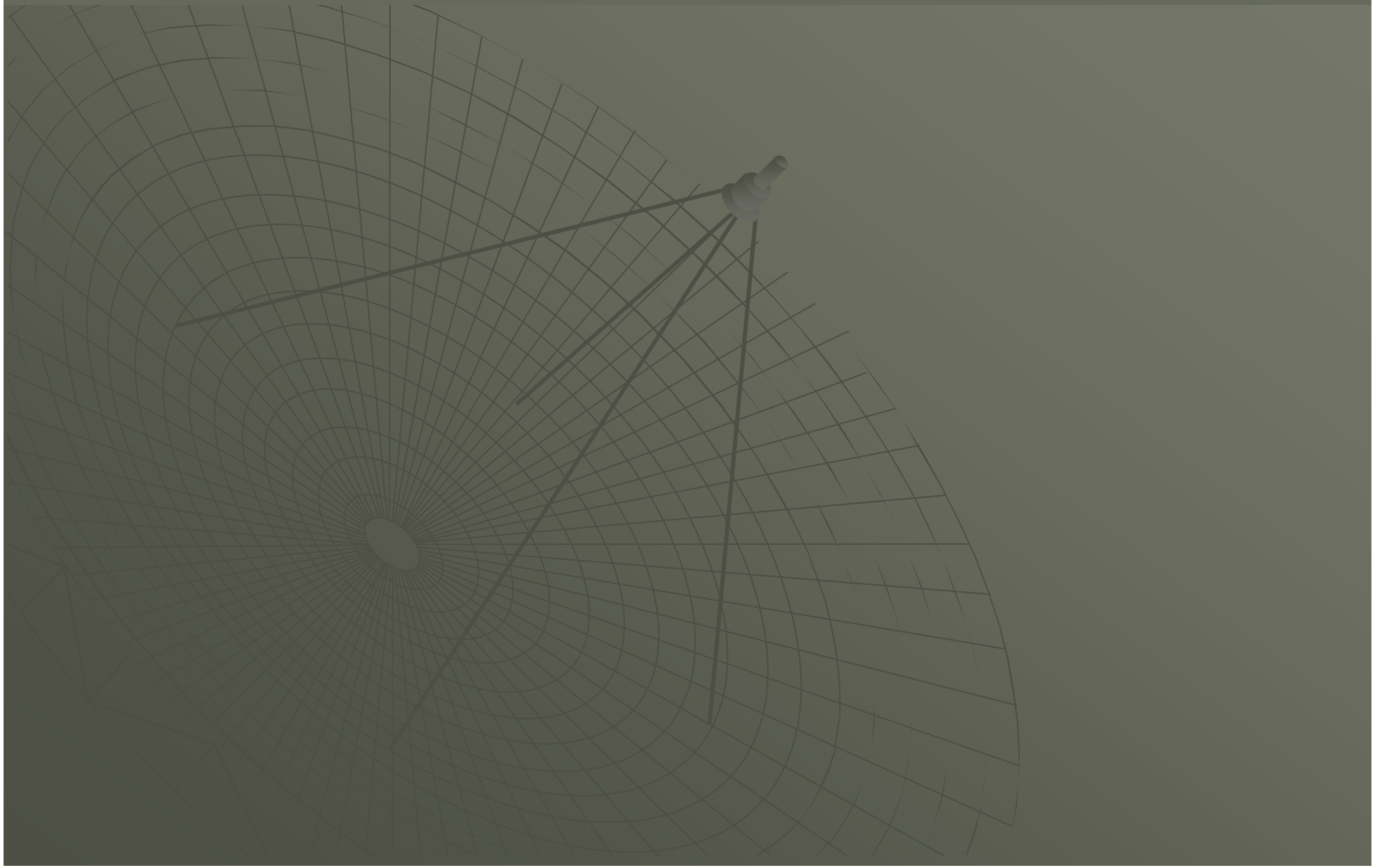
Block Cipher Modes

- **An Authentication Mode**
- **SP 800-38 B** ***Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*** **– (May 2005).**
- **An Authenticated Encryption Mode**
- **SP 800-38 C** ***Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality*** **– (May 2004).**

Block Cipher Modes

- **A High-Throughput Authenticated Encryption Mode**
- **SP 800-38 D** ***Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*** **– (Nov. 2005).**
- **A Confidentiality Mode Designed for Storage Devices**
- **SP 800-38 E** ***Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices*** **– (Jan. 2010).**

Digital Signatures



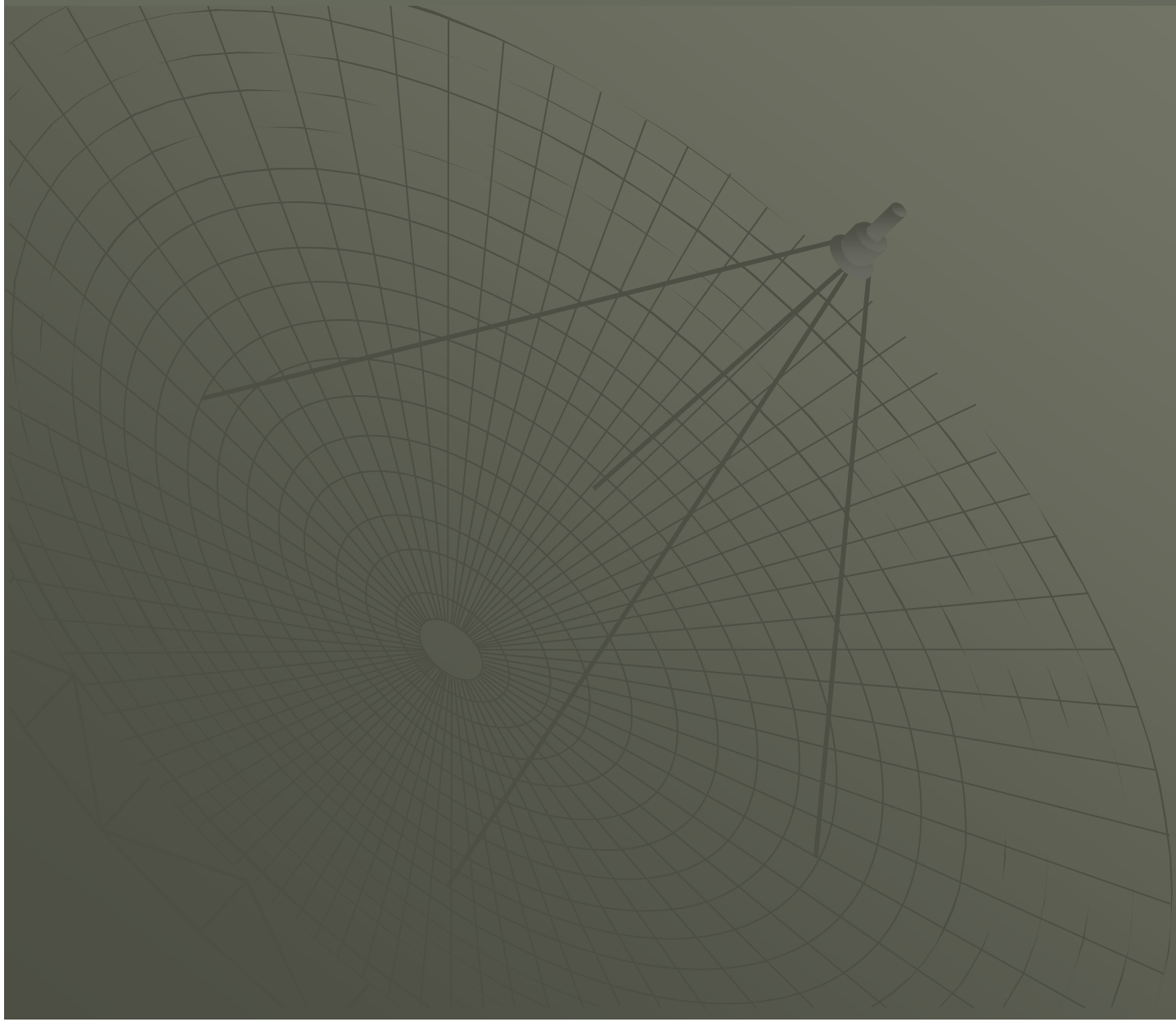
Digital Signatures

- **Approved algorithms for generating and verifying digital signatures: DSA, RSA, ECDSA**
- **FIPS 186-3**, ***Digital Signature Standard (DSS)*** **– (Jun. 2009).**
- **SP 800-89**, ***Recommendation for Obtaining Assurances for Digital Signature Applications*** **- (Nov. 2006).**
- **SP 800-102**, ***Recommendation for Digital Signature Timeliness*** **- (Sep. 2009).**
- **SP 800-106**, ***Randomized Hashing for Digital Signatures*** **- (Feb. 2009).**

Digital Signatures

- Approved algorithms for generating and verifying digital signatures: DSA, RSA, ECDSA
- FIPS 186-3, *Digital Signature Standard (DSS)* – (Jun. 2009).
- FIPS 186-3 indicates that the RSA digital signature algorithm, as specified in ANSI X9.31 and PKCS #1 and the ECDSA digital signature algorithm, as specified in ANSI X9.62-2005 , may be used for digital signature generation and verification.

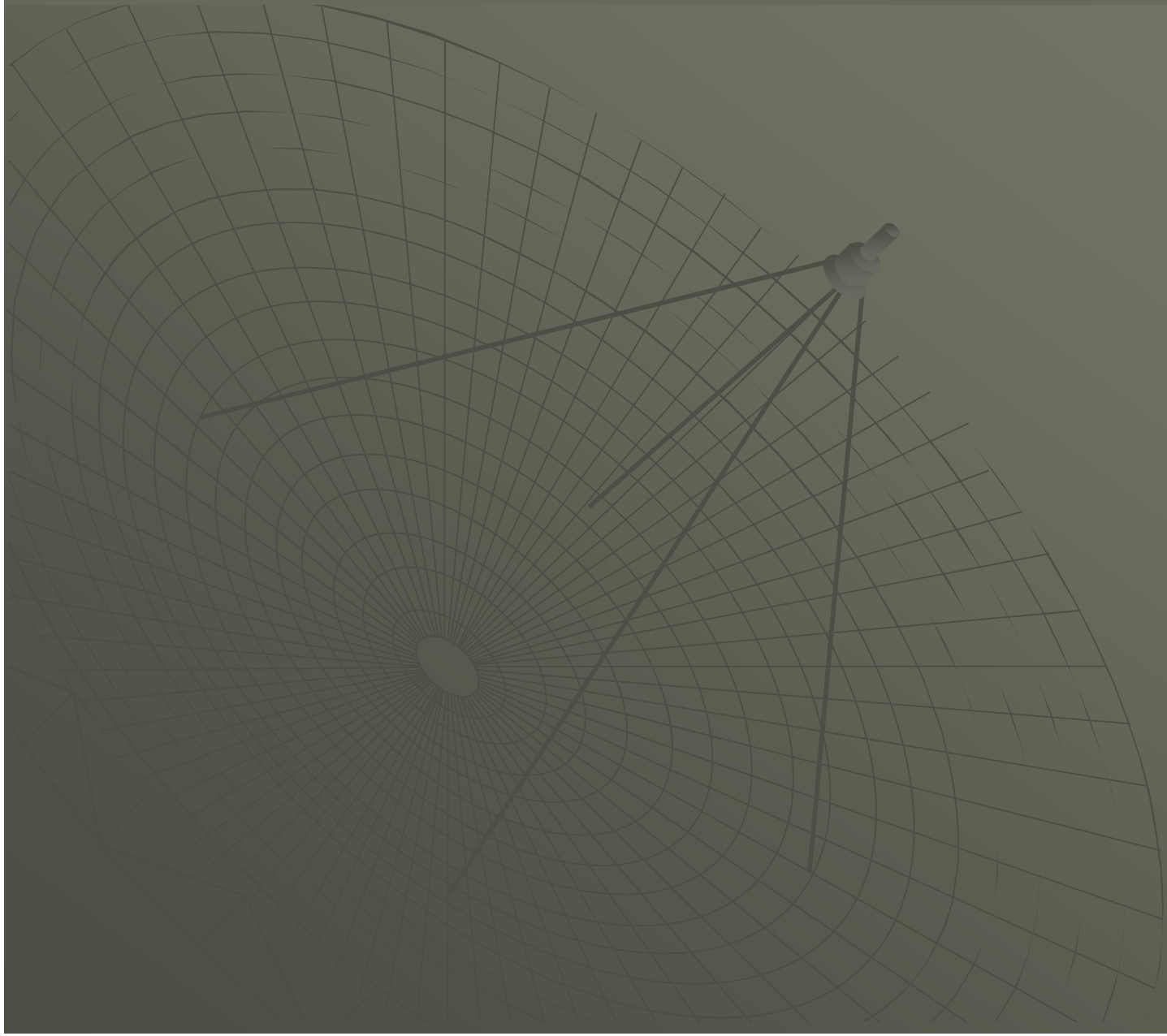
Entity Authentication



Entity Authentication

- **FIPS 196**, ***Entity Authentication Using Public Key Cryptography*** **– (Feb. 1997)**

Message Authentication

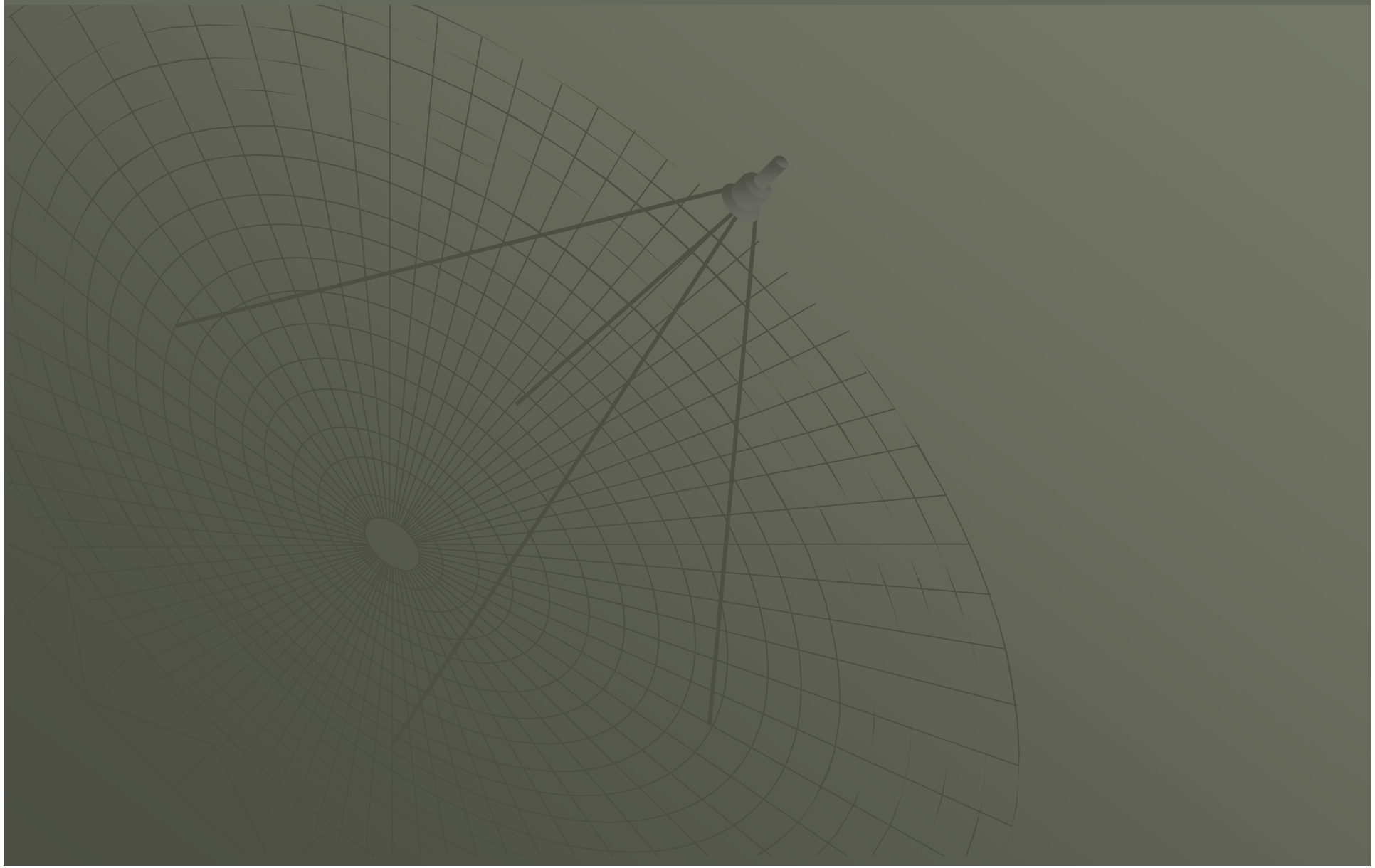


Message Authentication

- **Message Authentication Code (MAC or DAC)**
- **FIPS 113**, ***Computer Data Authentication*** **– (May 1985).**

- **Keyed-Hash Message Authentication Code (HMAC)**
- **FIPS 198-1**, ***The Keyed-Hash Message Authentication Code (HMAC)*** **– (Jul. 2008).**

Secure Hashing



Secure Hashing

Approved algorithms for generating a condensed representation of a message (message digest):

- FIPS 180-3, Secure Hash Standard (SHS), - (Oct. 2008). FIPS 180-2 (Aug. 2002)
  - SHA-1
  - SHA-2 (Mar. 2006): (SHA-224, SHA-256, SHA-384, SHA-512).
- SP 800-106, Randomized Hashing for Digital Signatures – (Feb. 2009).
- SP 800-107, Recommendation for Applications Using Approved Hash Algorithms – (Feb. 2009).

Secure Hashing

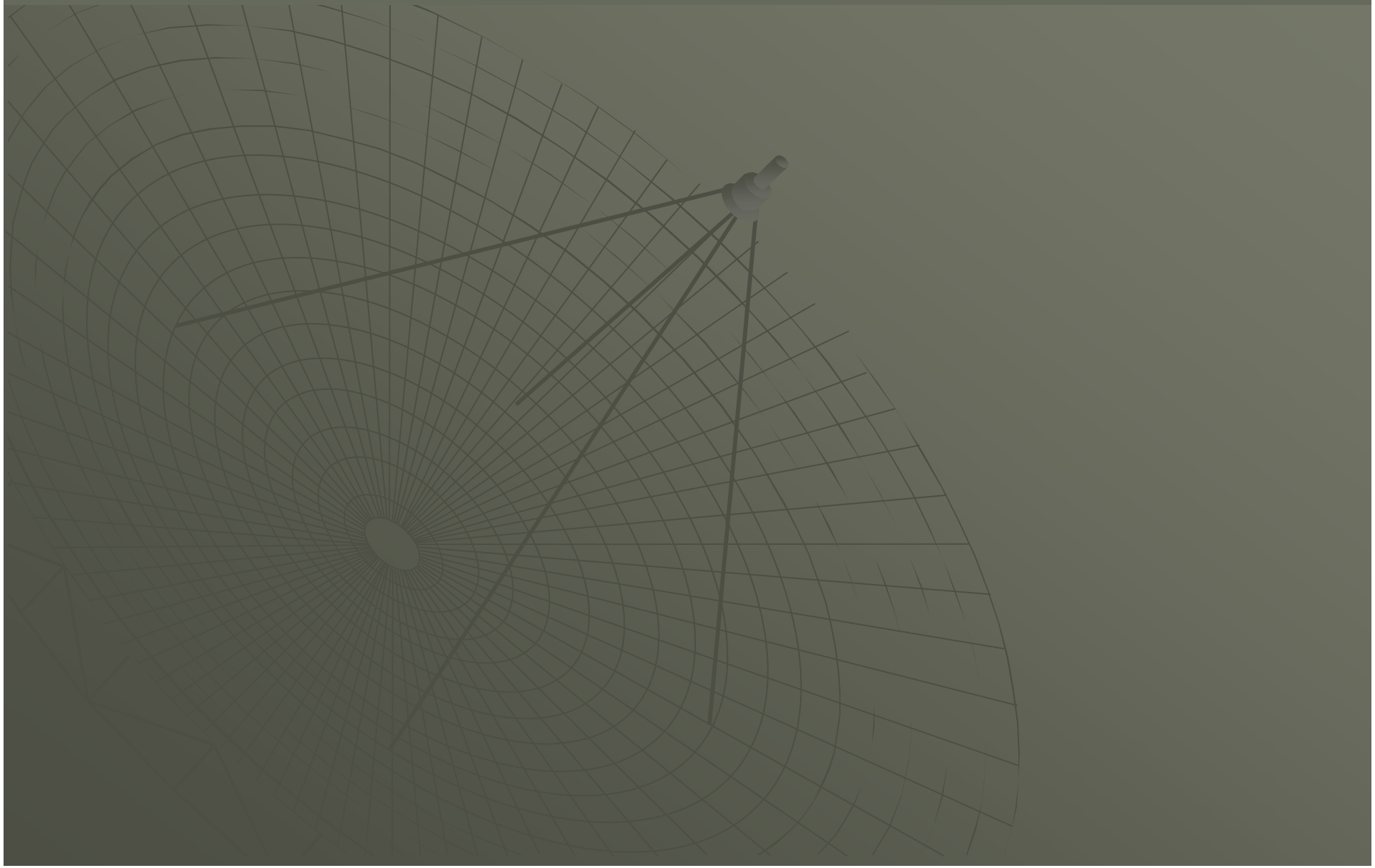
- **Cryptographic Hash Project**

On November 2, 2007 NIST has issued a Call for a New Cryptographic Hash Algorithm (SHA-3) Family to launch the hash algorithm competition.

Hash Algorithm Competition:

2007-2012

Key Management



Key Management

- **Key Management Project**
- **In 1997, NIST announced plans to develop a public key-based key management standard and solicited comments from the public.**
- **The first workshop was held in 2000.**
- **A second workshop was held in 2001 to discuss initial drafts of a Key Management Guideline and a Key Schemes document.**
- **April 13, 2009: NIST announced a Key Management Workshop.**

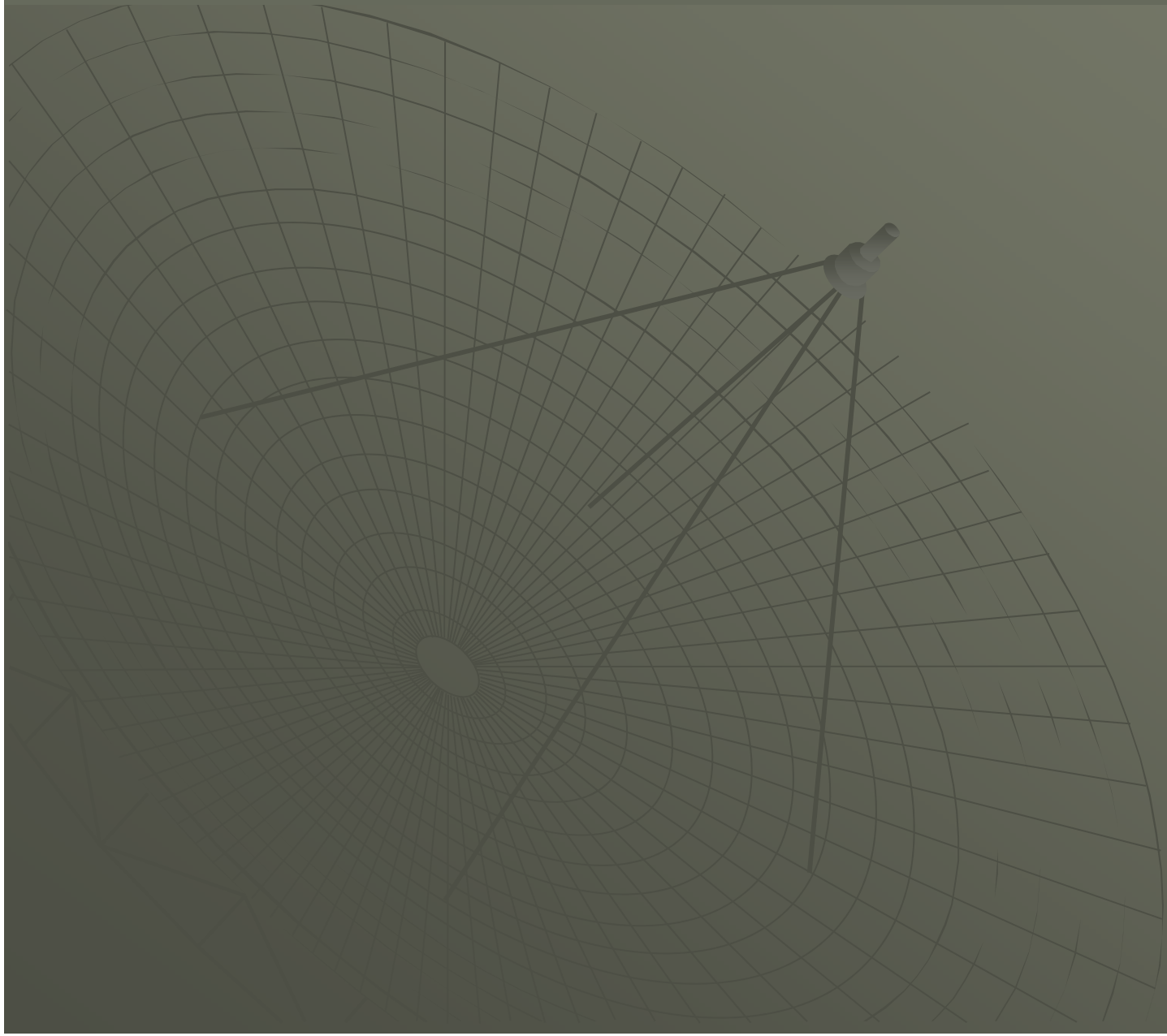
Key Management

- **Key Management Guideline**
- **SP 800-57 Part 1**, ***Recommendation for Key Management - Part 1: General (Revised)*** **- (Aug. 2005, Mar. 2007 updated).**
- **SP 800-57 Part 2**, ***Recommendation for Key Management - Part 2: Best Practices for Key Management Organizations*** **- (Mar. 2007).**
- **SP 800-57 Part 3 DRAFT**, ***Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance*** **- (Oct. 2008 DRAFT).**

Key Management

- **Key Schemes**
- **SP 800-56A**, ***Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*** **- (Mar. 2007 updated).**
- **SP 800-56B DRAFT,** ***Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography*** **- (Dec. 2008 Draft).**

Key Derivation Functions

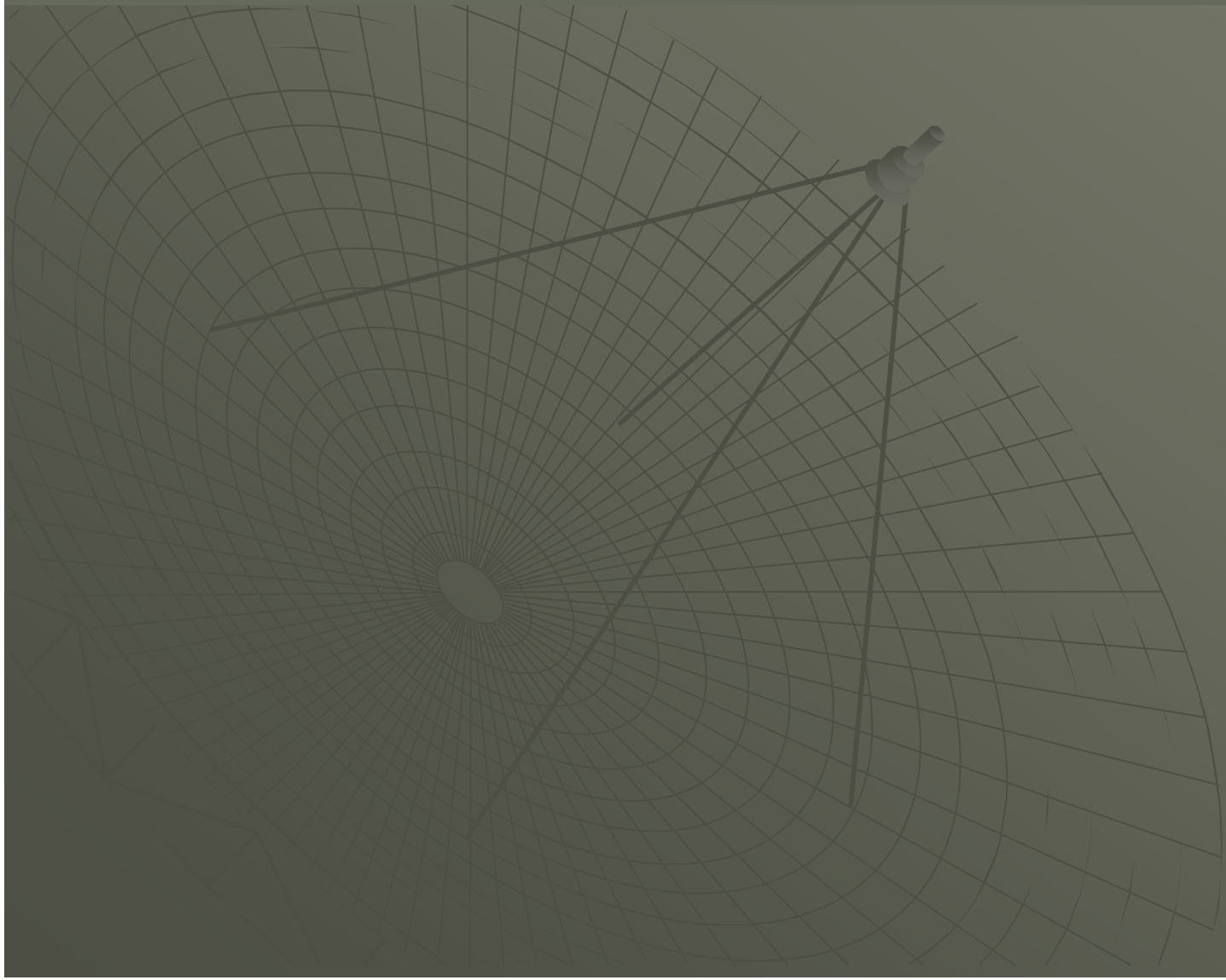


Key Derivation Functions

- **SP 800-108**, ***Recommendation for Key Derivation Using Pseudorandom Functions*** **- (Nov. 2008)**

  - Recommendation specifies techniques for the derivation of additional keying materialfrom a secret cryptographic key using pseudorandom functions.

Password Usage and Generation

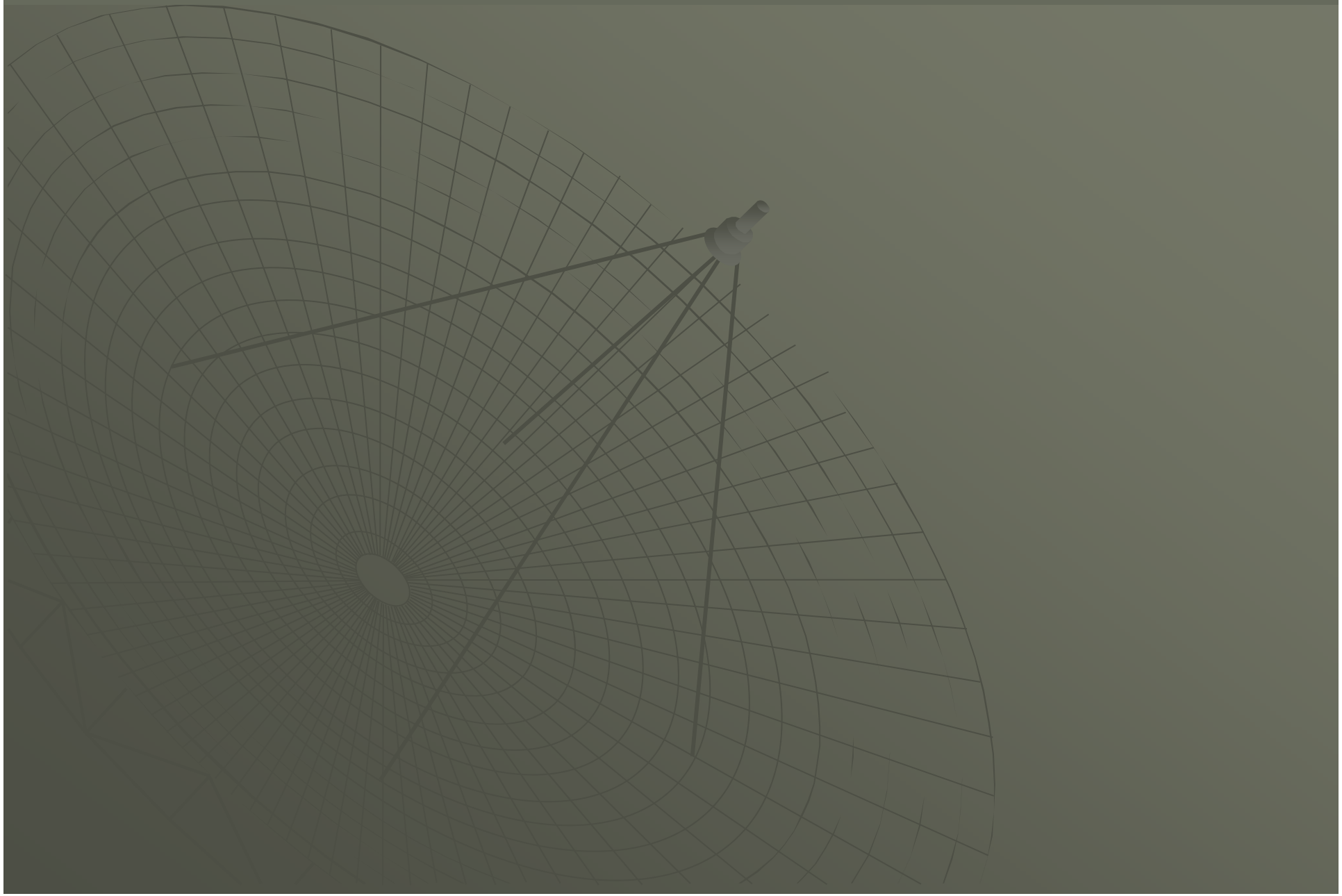


Password Usage and Generation

- **Password Usage**
- **FIPS 112**, ***Password Usage*** **(May 1985).**

- **Automated Password Generator**
- **FIPS 181, Automated Password Generator - (Oct. 1993).**

Random Number Generation



Random Number Generation

Generally-speaking, there are two types of random number generators (RNGs):

- RNGs based on Deterministic Random Bit Generators (DRBGs), also known as Pseudorandom Number Generators, and
- RNGs based on Non-deterministic Random Bit Generators (NRBGs), also known as "True" Random Number Generators.

Currently, there exists several Approved DRBGs, and no Approved NRBGs.

Random Number Generation

- **Deterministic Generators**
- **FIPS 186-2**, Digital Signature Standard (DSS), defines two deterministic techniques for generating numbers. (Appendices 3.1 and 3.2 and Change Notice #1) - (Jan. 2000).
  Note: FIPS 186-2 has been superceded by FIPS 186-3 - (Jun. 2009).

- **ANSI X9.31**, Appendix A.2.4.
  = **ANSI X9.17**, Appendix C.
- **ANSI X9.62-1998**, Annex A.4.

Random Number Generation

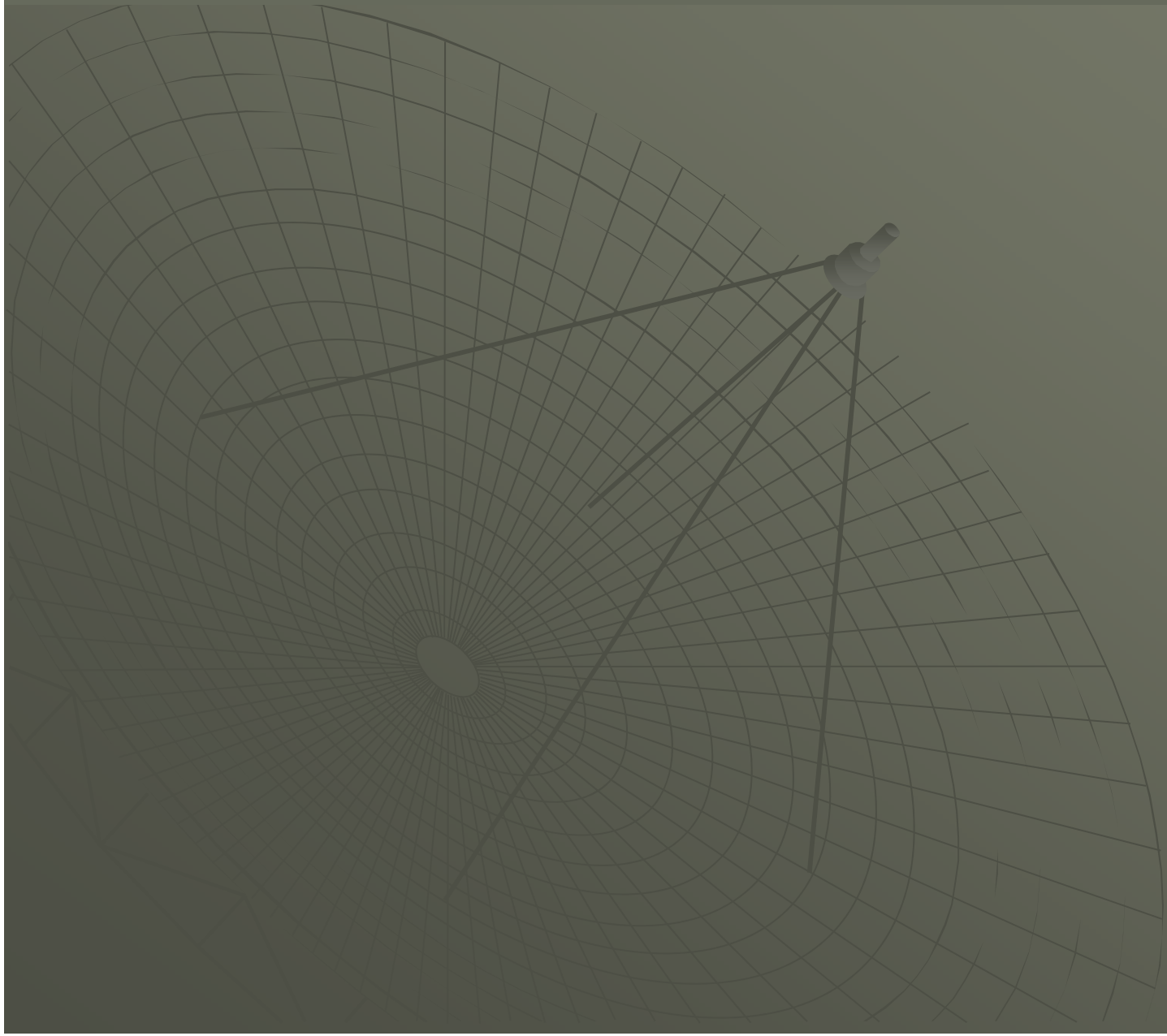
- **Deterministic Generators**
- **SP 800-90**, ***Recommendation for Random Number Generation Using Deterministic Random Bit Generators*** **– (Mar. 2007)**

Random Number Generation

- **RNG Testing**
- **SP 800-22, Rev. 1**, ***A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*** **– (Aug. 2008)**
- **NIST has published an ITL Bulletin that summarizes SP 800-22.**
- **NIST maintains a general web page on Random Number Generation and Testing:**

  http://csrc.nist.gov/groups/ST/toolkit/rng/index.html

Implementation Guideline

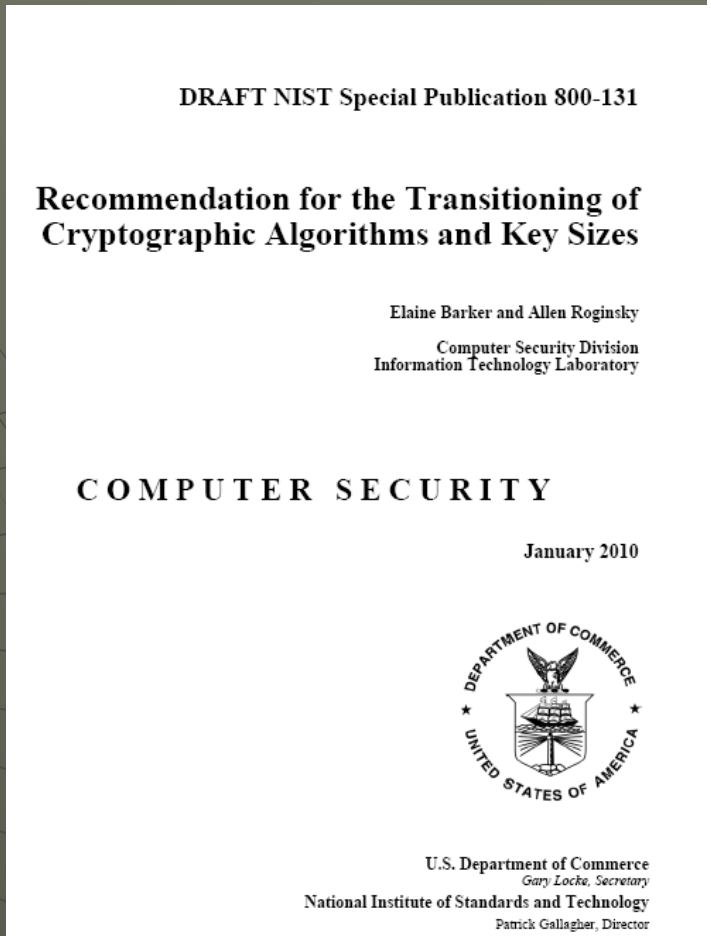


Implementation Guideline

- **Guideline for Implementing Cryptography**
- **SP 800-21-1, Second Edition, *Guideline for Implementing Cryptography in the Federal Government* – (Dec. 2005).**

SP 800-131

Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes



DRAFT NIST Special Publication 800-131

Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes

Elaine Barker and Allen Roginsky

Computer Security Division
Information Technology Laboratory

COMPUTER SECURITY

January 2010

U.S. Department of Commerce
Gary Locke, Secretary
National Institute of Standards and Technology
Patrick Gallagher, Director

Сравнительная стойкость криптоалгоритмов и сроки их действия

Bits of security	Symmetric key algorithms	FFC (DSA, D-H, MQV)	IFC (RSA)	ECC (ECDSA)
80 (до 2010 г.)	2TDEA, SKIPJACK,	$L = 1024$ $N = 160$	$k = 1024$	$f = 160\text{-}223$
112 (до 2030 г.)	3TDEA	$L = 2048$ $N = 224$	$k = 2048$	$f = 224\text{-}255$
128 (после 2030 г.)	AES-128	$L = 3072$ $N = 256$	$k = 3072$	$f = 256\text{-}383$
192	ES-192	$L = 7680$ $N = 384$	$k = 7680$	$f = 384\text{-}511$
256	AE	$L = 15360$ $N = 512$	$k = 15360$	$f = 512+$

после 2030 г.

Сравнительная стойкость криптоалгоритмов и сроки их действия

Bits of security	Symmetric key algorithms	FFC (DSA, D-H, MQV)	IFC (RSA)	ECC (ECDSA)
80 (до 2010 г.)	2TDEA, SKIPJACK,	$L = 1024$ $N = 160$	$k = 1024$	$f = 160\text{-}223$
112 (до 2030 г.)	3TDEA	$L = 2048$ $N = 224$	$k = 2048$	$f = 224\text{-}255$
128 (после 2030 г.)	AES-128	$L = 3072$ $N = 256$	$k = 3072$	$f = 256\text{-}383$
192	AES-192	$L = 7680$ $N = 384$	$k = 7680$	$f = 384\text{-}511$
256	AES-256	$L = 15360$ $N = 512$	$k = 15360$	$f = 512+$

Российские криптографические стандарты

Сравнительная стойкость криптоалгоритмов и сроки их действия

Bits of security	Symmetric key algorithms	FFC (DSA, D-H, MQV)	IFC (RSA)	ECC (ECDSA)
80 (до 2010 г.)	2TDEA, SKIPJACK,	$L = 1024$ $N = 160$	$k = 1024$	$f = 160\text{-}223$
112 (до 2030 г.)	3TDEA	$L = 2048$ $N = 224$	$k = 2048$	$f = 224\text{-}255$
128 (после 2030 г.)	AES-128	$L = 3072$ $N = 256$	$k = 3072$	$f = 256\text{-}383$
192	AES-192	$L = 7680$ $N = 384$	$k = 7680$	$f = 384\text{-}511$
256	AES-256	$L = 15360$ $N = 512$	$k = 15360$	$f = 512+$

ГОСТ 28147-89

ГОСТ Р 34.10-94
$L = 509\text{-}512$ или $1020\text{-}1024$,
$N = 254\text{-}256$

ГОСТ Р 34.10-2001
$f = 256$

Hash Function Security Strengths for Cryptographic Applications

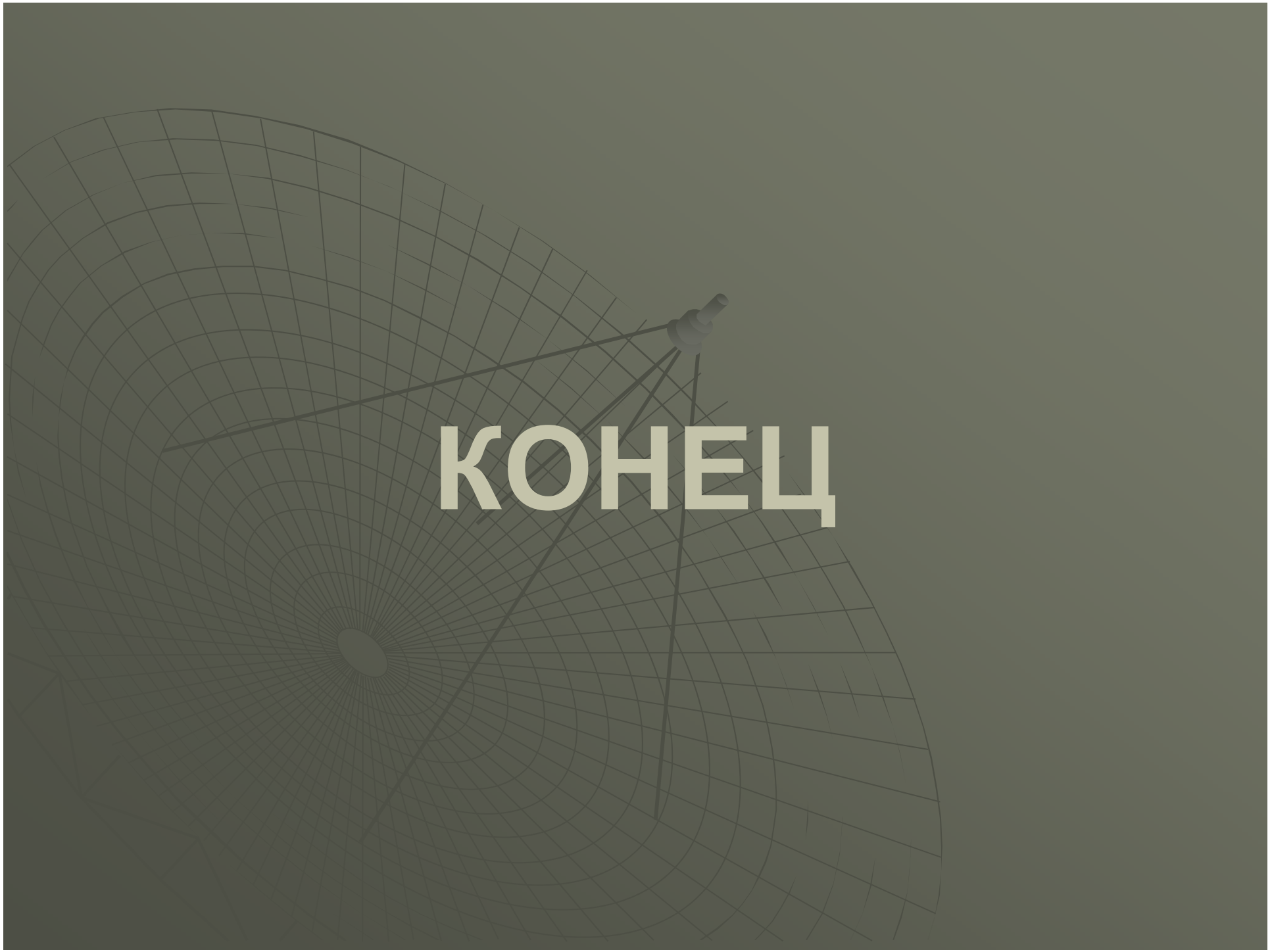
Bits of Security	Digital Signatures and hash-only applications	HMAC	Key Derivation Functions[2]	Random Number Generation[3]
80 (до 2010 г.)	SHA-1, SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512)	SHA-1, SHA-2	SHA-1, SHA-2	SHA-1, SHA-2
112 (до 2030 г.)	SHA-224, SHA-256, SHA-384, SHA-512	SHA-1, SHA-2	SHA-1, SHA-2	SHA-1, SHA-2
128 (после 2030 г.)	SHA-256, SHA-384, SHA-512	SHA-1, SHA-2	SHA-1, SHA-2	SHA-1, SHA-2
192	SHA-384, SHA-512	SHA-2	SHA-2	SHA-2
256	SHA-512	SHA-256, SHA-384, SHA-512	SHA-256, SHA-384, SHA-512	SHA-256, SHA-384, SHA-512

FFC Parameter Size Sets

FFC Parameter Set Name	FA (до 2010 г.)	FB (до 2030 г.)	FC (после 2030 г.)
Bit length of field order p (i.e., $\lceil \log_2 p \rceil$)	1024	2048	2048
Bit length of subgroup order q (i.e., $\lceil \log_2 q \rceil$)	160	224	256
Minimum bit length of the hash function output	160	224	256
Minimum MAC key size (for use in key confirmation)	80	112	128
Minimum *MacLen* (for use in key confirmation)	80	112	128

ECC Parameter Size Sets

ECC Parameter Set Name	EA (до 2010 г.)	EB (до 2030 г.)	EC (после 2030 г.)	ED	EE
Bit length of ECC subgroup order *n* (i.e., $[\log_2 n]$)	160-223	224-255	256-383	384-511	512+
Maximum bit length of ECC cofactor *h*	10	14	16	24	32
Minimum bit length of the hash function output	160	224	256	384	512
Minimum MAC key size (for use in key confirmation)	80	112	128	192	256
Minimum *MacLen* (for use in key confirmation)	80	112	128	192	256


КОНЕЦ