Encryption Protection of Data-at-Rest

Alexander (Sandy) Stewart
Sun MicroSystems
1 StorageTek Drive, Louisville CO 80028-2121
Phone:+1-303-673-2775 FAX: +1-303-661-5743
E-mail: alexander.stewart@sun.com

Presented at the THIC Meeting at the National Center for Atmospheric Research, 1850 Table Mesa Drive, Boulder CO 80305-5602

July 18-19, 2006

The First Rule of Cryptography

The First Rule of Cryptography

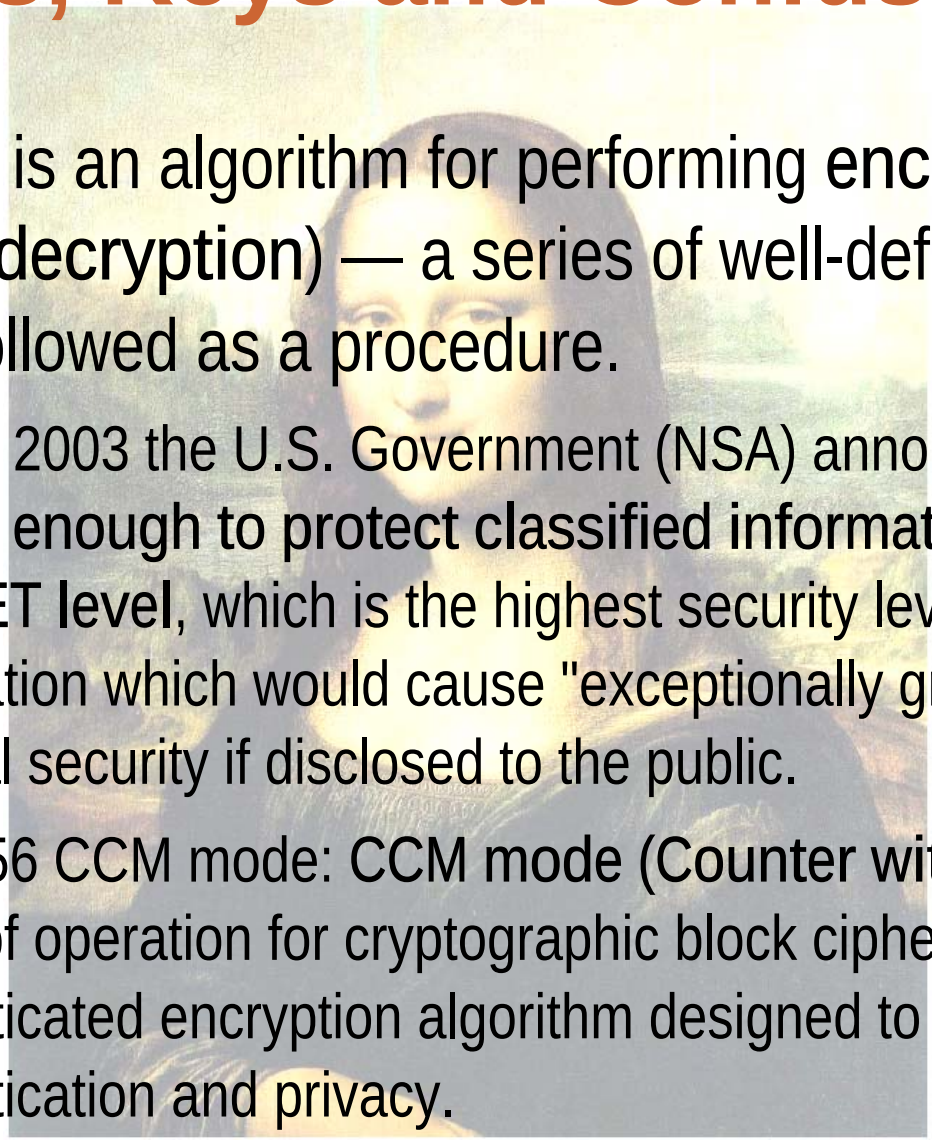
You can’t talk about cryptography without showing a picture of the Enigma machine

The First Rule of Cryptography

You can't talk about cryptography without showing a picture of the Enigma machine

The designers of Enigma thought it couldn't be broken……

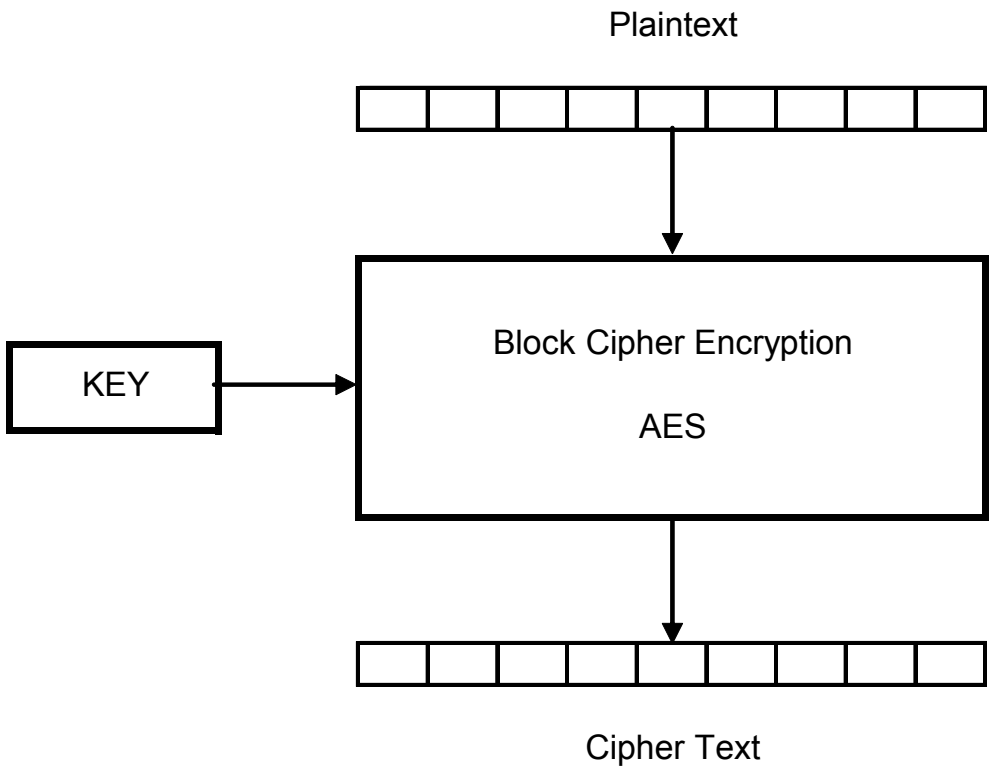
Ciphers, Keys and Confusion



- A **cipher** is an algorithm for performing **encryption** (and the reverse, **decryption**) — a series of well-defined steps that can be followed as a procedure.
  - in June 2003 the U.S. Government (NSA) announced that **AES is secure enough to protect classified information up to the TOP SECRET level**, which is the highest security level and defined as information which would cause "exceptionally grave damage" to national security if disclosed to the public.
  - AES-256 CCM mode: **CCM mode (Counter with CBC-MAC)** is a mode of operation for cryptographic block ciphers. It is an authenticated encryption algorithm designed to provide both authentication and privacy.

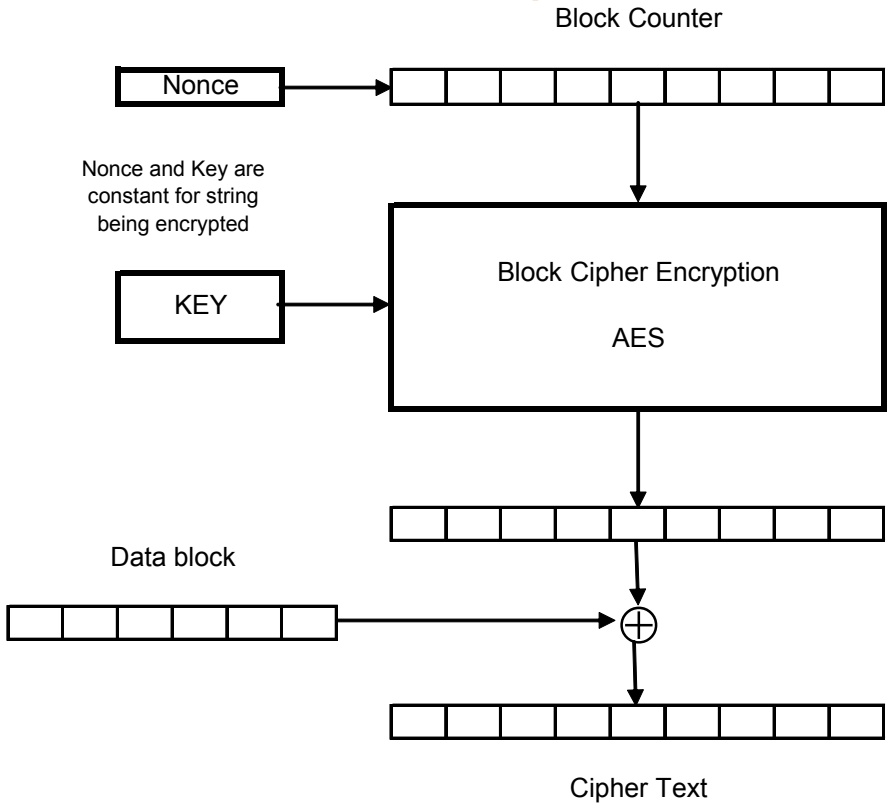
CCM mode (Counter with CBC-MAC)

AES Block Cipher Encryption
Typically performed using multiple iterations of a simpler algorithm (round)



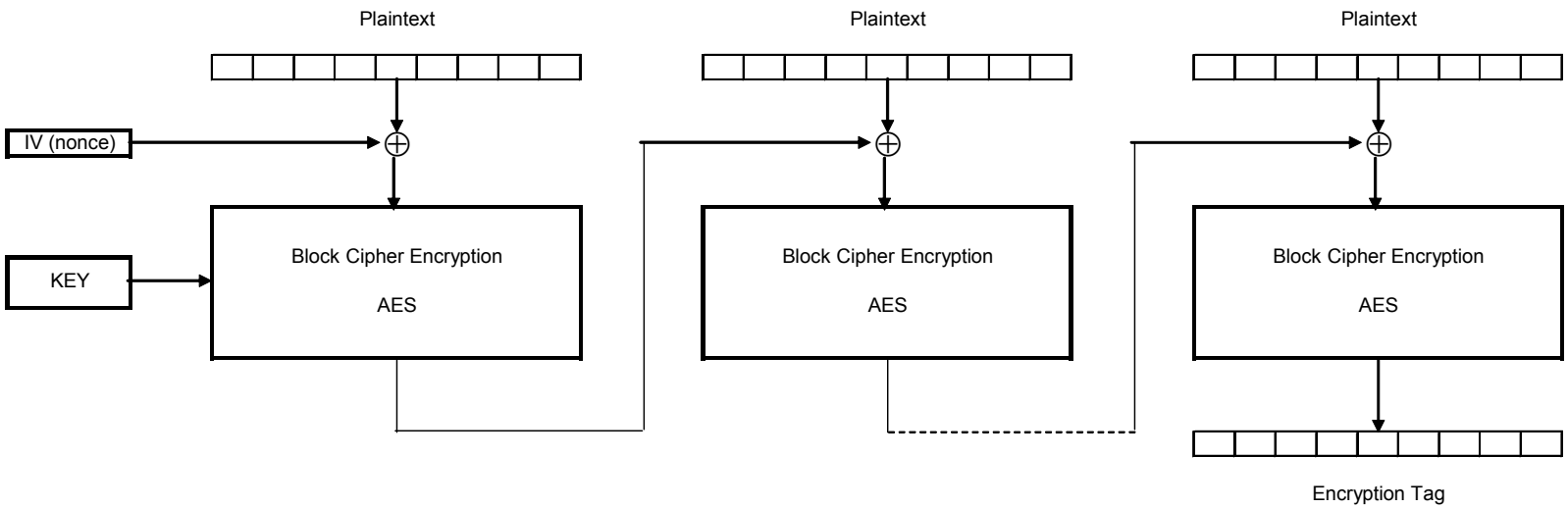
CCM mode (Counter with CBC-MAC)

Counter Mode turns a block cipher into a stream cipher



CCM mode (Counter with CBC-MAC)

Cipher Block Chaining is used to create the Encryption Tag



Plaintext input includes Encryption Header as well as payload data

Ciphers, Keys and Confusion

- The encrypting procedure is varied depending on the **key**, which changes the detailed operation of the algorithm.
  - Key size, ***ie*** the size of key used to encrypt a message. As the key size increases, so does the complexity of brute force search to the point where it becomes infeasible to crack encryption directly.
  - Keys must be strong – i.e. random and hard to guess
  - Keys must be protected – steal the key you can steal the data
  - Brute force attack: if you could try a key every ns, it would take 3.67×10^{60} years to try all potential combinations

Encryption

Defining the Principles of the Next Generation of Data Protection

At Creation

In Band Appliances

In Device

Data Encryption

Three Options

Host/Server

- Server-based via the operating system or using cryptographic hardware

In-Band

- Various “appliances” that offer technologies that encrypt the data stream that is going over network interconnects

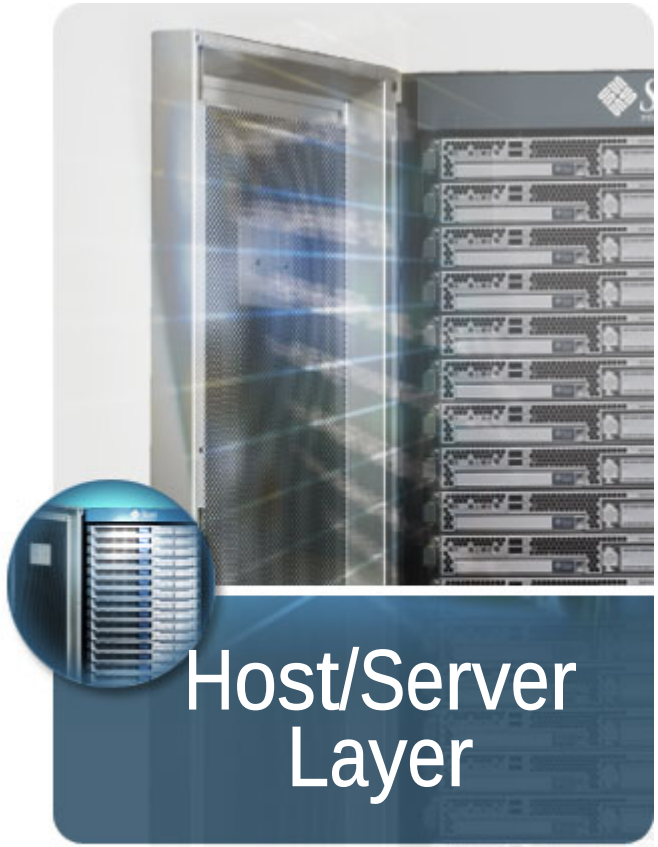
In Device

- Encryption of data as it resides on the tape cartridges protects against unauthorized access to data if tapes are lost or stolen

Encrypting at Data Creation

Server-Based Encryption Solutions

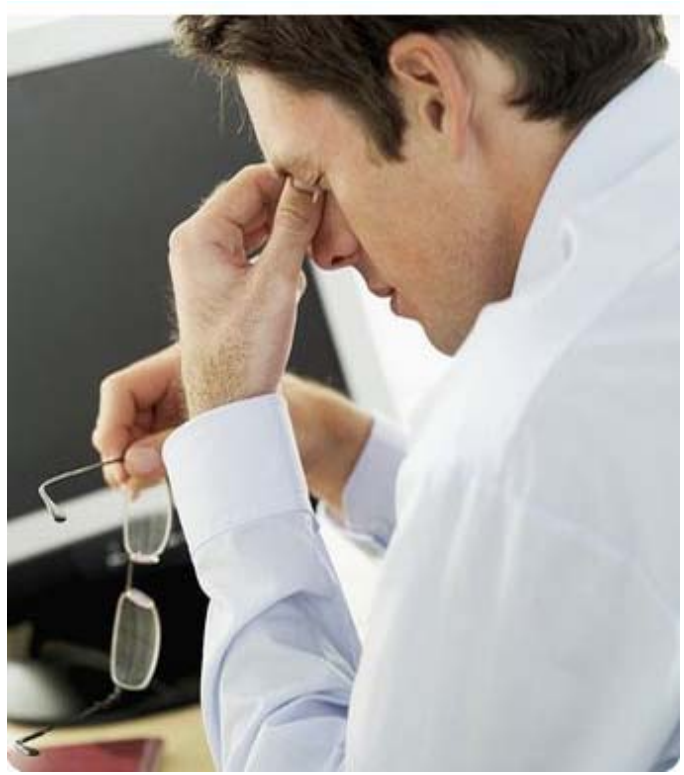
- Data encrypted the moment it's created, providing the first possible level of data security
- There is little chance of encrypted data being intercepted, either accidentally or maliciously
- If data is intercepted, encryption renders it unreadable
- Bottom line: Host-based encryption is a good fit for sensitive data as it travels through the network and when TCO is less important



Encrypting Data at Creation

Server-Based Encryption Challenges

- Legacy operating infrastructure needs to be changed to implement this method
- Once data is encrypted, it can't be compressed
- Encryption can increase data processing overhead in legacy hardware by as much as 40%



In-Band Encryption

In-band Appliance-based Solutions

- Sun Client Services can provide customers with secure data encryption solutions today using in-band appliances
- A typical engagement includes:
  - > Security risk analysis
  - > Encryption vendor selection
  - > Vendor interoperability and proof of concept
  - > Solution implementation

Bottom Line: Easy to implement but possible to bypass. Suited as a short-term expedient for localized encryption solutions

In-Band Encryption

Appliance-based Challenges

- Encourages mirrored devices, as a single point of failure blocks access to data
- Oriented toward a multi-tiered security model
- Provides a method of recovering data in case of a complete meltdown of the encryption system, as long as keys have been saved to portable storage

Bottom Line: Easy to implement but possible to bypass. Suited as a short-term expedient for localized encryption solutions

Encryption In Device

In-device Based Encryption Solutions

- Data can be encrypted on a tape or disk drive device, making it easy to validate and eliminating the performance penalty on the server
- Most secure solution
- It is easiest to implement

Bottom line: This is a good fit for heterogeneous environments; inherently secure, reduces complexity, risk, and total cost of ownership

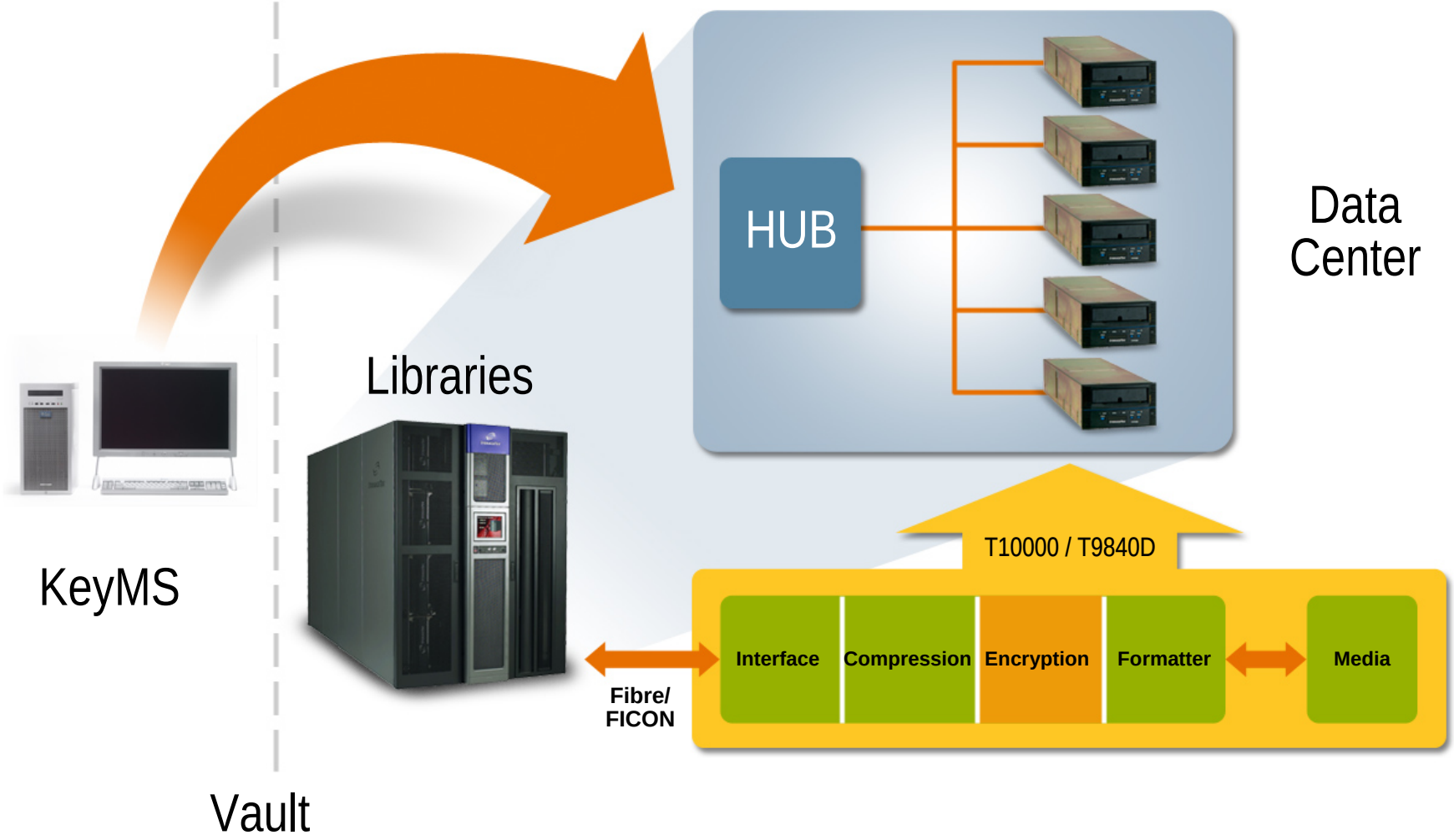
Three Key Elements Needed for Data Encryption on Tape or Disk

"Crypto-Ready" Drive

Key Management Station

Key Transmission

Tape Encryption Conceptual Overview



Tape Encryption Design Approach

- Add encryption engine between the Compression and the Formatter functions
  - Encrypted data is highly randomized so encryption must be done post-compression to retain the benefits of compression

CCM and GCM are IEEE P1619.1 recommended modes for tape

  - CCM mode is already FIPS approved
  - Both allow authentication of encryption header – including Key ID

- Encryption Overhead: 100bytes, insignificant for typical tape block sizes: 24K to 256K and growing

What is on the Tape?

- Encrypted package written on the tape comprises:
  - Encryption header
    - Key ID
    - Non-repeating nonce
  - Encrypted data
  - Encryption tag
    - Used with the encryption header to authenticate the data
- THE KEY IS NOT PRESENT ON THE TAPE

Sample Encrypted data

Byte	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
0000000	00	00	00	00	00	00	00	00	7a	b0	22	b0	33	b0	44	b0
0000016	00	b0	00	b0	91	00	00	48	00	1e	02	b1	03	b1	04	b1
0000032	05	b1	06	b1	07	b1	08	b1	01	b2	02	b2	03	b2	04	b2
0000048	05	b2	06	b2	07	b2	08	b2	34	ec	36	f3	1d	6e	6e	88
0000064	35	ca	ec	f4	e6	1e	34	c1	c5	38	2e	f7	3a	d9	9e	e9
0000080	0e	e7	62	7b	b8	68	f7	0b	b4	4e	5a	4a	aa	0f	27	94
0000096	ec	45	f6	81	47	af	a0	13	fd	a2	5c	26	23	47	fb	4a
0000112	9f	8b	82	65	e2	58	37	bd	cc	90	12	e6	db	3c	64	32
0000128	98	89	41	6f	70	b9	8d	5b	c1	32	e5	0b	56	3d	45	94
0000432	00	00	00	00	00	00	00	00	7a	b0	22	b0	33	b0	44	b0
0000448	00	b0	00	b0	94	00	00	48	00	1e	02	b1	03	b1	04	b1
0000464	05	b1	06	b1	07	b1	08	b1	01	b2	02	b2	03	b2	04	b2
0000480	05	b2	06	b2	07	b2	08	b2	e4	6d	94	d6	99	10	ba	d6
0000496	01	70	27	ee	08	0a	a1	7c	c8	1b	61	cc	dd	0f	d3	1f
0000512	69	d6	5f	40	37	d7	37	2a	d4	a0	0a	a5	86	53	8c	d5
0000528	90	36	2a	a3	47	7b	cb	82	01	ee	53	b4	d2	15	5b	cf
0000544	34	c4	67	67	1c	46	a7	ab	bc	f5	ed	6e	4d	34	e2	fd
0000560	43	29	89	48	ce	ec	4e	13	49	d0	7e	ef	eb	e3	ff	d2
0000576	00	00	00	00	00	00	00	00	7a	b0	22	b0	33	b0	44	b0
0000592	00	b0	00	b0	95	00	00	48	00	1e	02	b1	03	b1	04	b1
0000608	05	b1	06	b1	07	b1	08	b1	01	b2	02	b2	03	b2	04	b2
0000624	05	b2	06	b2	07	b2	08	b2	bd	ca	05	ec	a2	20	1b	3f
0000640	26	72	27	ef	2e	dc	c7	42	da	3b	41	a6	3b	e1	32	f7
0000656	62	7e	d1	96	76	ad	5d	9b	cd	da	6a	74	c3	34	28	e0
0000672	e4	72	bf	75	ea	cc	22	3a	d3	b4	4b	d7	ce	e0	1f	fd
0000688	ac	b8	3a	d4	18	29	68	9a	d4	f7	2b	bc	5b	13	3e	28
0000704	14	d5	9f	8e	ce	59	43	80	39	99	92	fe	c9	dd	b3	03
Legend			nonce				Key ID				user data				tag & CRC	

The challenge of disk…..

- Typical disk drive solutions use fixed 512-byte block length formats
- Does not allow added overhead
  - Nonce must be derived from block address
  - Key must be pre-assigned per disk or per partition and cannot be changed
  - No ability to provide authentication

Key Handling

The encryption algorithms described provide solid security and the only practical way to attack data is to steal the key

- Keys must be protected at generation
  - True random number generator for key value
- Only authorized users may handle keys
  - Robust identity management
  - Quorum key management
- Keys must be protected in transmission
  - Never expose key values in-the-clear
  - Key values in transit must be protected (e.g. by encryption)
  - Protection against play-back attacks

Key Management Imperatives

Key Management Station

- Enforces Identity and Role Management
- Assured backup of every key and its associated key ID
- Provides a user-friendly GUI that
  - Facilitates the user's Security Policy and procedures
  - Allows the user to create, assign and revoke encryption keys
  - Supports the Device keys used to obscure Media Keys
  - Supports key assignment across all encryption agents used in the data fabric including 3rd Party solutions
  - Supports ILM by time-based key expiration