

Encryption Controls

Anita Zinzuvadia
Information Technology Controls Division

Encryption controls

- ▶ How they came to be what they are today.
 - ▶ Negative list vs. positive list controls
- ▶ Exclusions, carve outs, exceptions

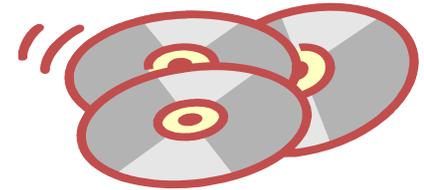
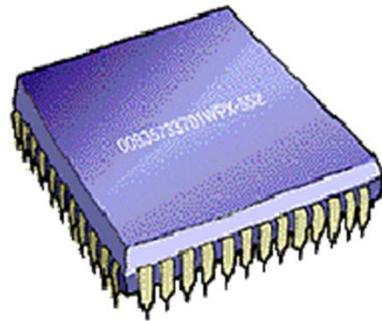


NOT encryption....

- ▶ Encrypted data
 - ▶ E.g., Music/video/multimedia (we control the software and equipment that encrypts/decrypts, not the content)
- ▶ Data Compression
- ▶ Coding techniques for reliable transmission (e.g. CDMA, parity bits)
- ▶ Note 4
- ▶ Publicly available (free)
- ▶ Service - SaaS



What are Encryption Items?



Do I have an encryption item?

- ▶ Yes, if your item contains encryption
 - ▶ Yes, even if your item does not use the encryption
- ▶ Yes, if your item uses encryption from an external source -- such as:
 - ▶ operating system (OS) software
 - ▶ external library
 - ▶ third-party product
 - ▶ cryptographic processor



Things to look for

▶ Algorithms

- ▶ Advanced Encryption Standard (AES)
- ▶ Rivest, Shamir, and Adleman (RSA)
- ▶ Data Encryption Standard (DES)
- ▶ Elliptic Curve Cryptography

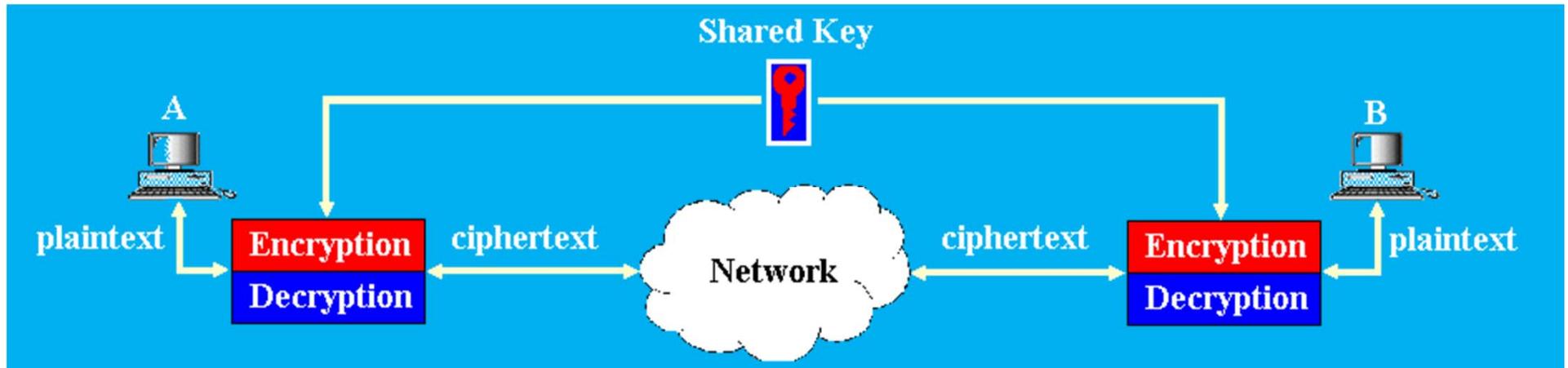


▶ Protocols

- ▶ IP Security (IPSec)
- ▶ Secure Socket Layer (SSL)
- ▶ WiFi (IEEE 802.11) /
WiMAX (IEEE 802.16)



Symmetric Encryption



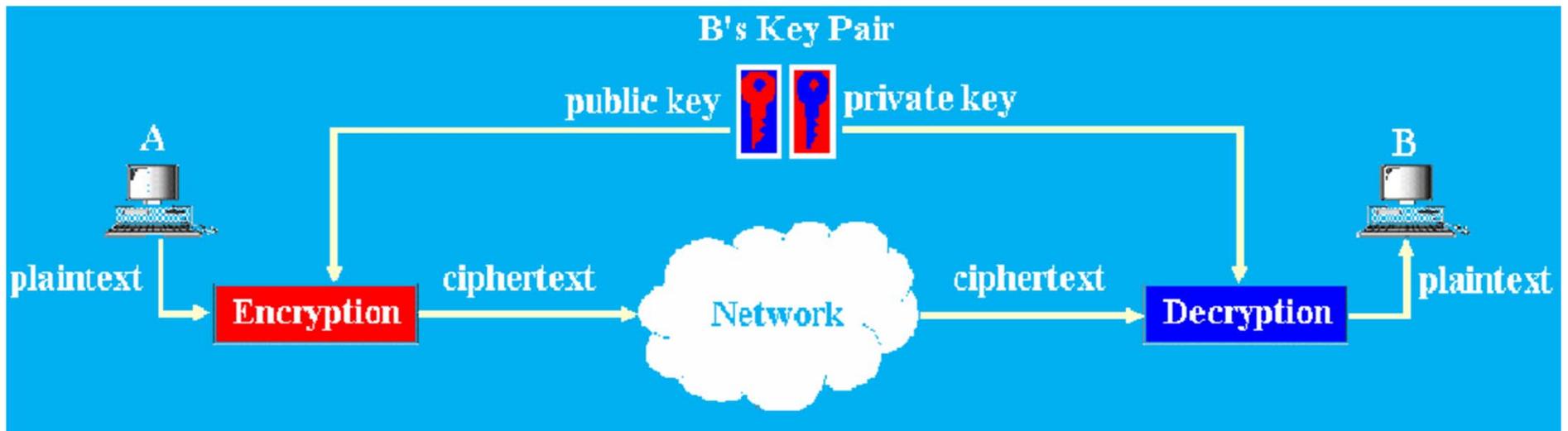
▶ Symmetric Algorithms

- ▶ DES – Data Encryption Standard
- ▶ 3DES – Triple-DES
- ▶ AES – Advanced Encryption Standard
- ▶ Blowfish
- ▶ IDEA
- ▶ RC4, RC5 and RC6

>56-bit key length symmetric encryption items are controlled for EI, NS, AT reasons.



Asymmetric Encryption



- ▶ Asymmetric algorithms
 - ▶ RSA
 - ▶ Elliptic Curve Cryptosystem (ECC)
 - ▶ Diffie-Hellman
 - ▶ El Gamal
 - ▶ Digital Signature Algorithm (DSA)
 - ▶ Knapsack

**>512-bit RSA / D-H and
>112-bit Elliptic Curve
asymmetric encryption
items are controlled for EI,
NS, AT reasons.**



Encryption items

- ▶ Publicly available
- ▶ Note 4
- ▶ Decontrol / <56/512/112
- ▶ Mass market Note 3
- ▶ License Exception ENC



Publicly available

- ▶ Certain publicly available encryption software is not subject to the EAR
- ▶ Generally includes source code eligible for TSU, related object code, or 'free' mass market items.
- ▶ Implemented January 7, 2011



Where does the item belong??

EAR99

- Note 4

5x992

- Decontrols
- Mass Market (Note 3)
- < 56/512/112 bit encryption

5x002

- ENC
-
- 

Not encryption

EAR99

Note 4 to Cat 5 Part 2

- ▶ The primary function is not:
 - ▶ “Information security”;
 - ▶ A computer, including operating systems, parts and components therefor;
 - ▶ Sending, receiving or storing information (except in support of entertainment, mass commercial broadcasts, digital rights management or medical records management); or
 - ▶ Networking (includes operation, administration, management and provisioning);

AND

- ▶ Encryption supports primary function
-



Note 4 examples

- ▶ Copyright protection, software licensing
- ▶ Games and gaming
- ▶ Household utilities and appliances
- ▶ Printing, reproduction, imaging and video recording or playback—not videoconferencing
- ▶ Business process modeling and automation (e.g., supply chain management, inventory, scheduling and delivery)
- ▶ Industrial, manufacturing or mechanical systems (e.g., robotics, heavy equipment, facilities systems such as fire alarm, HVAC)
- ▶ Automotive, aviation, and other transportation systems



Limited encryption

5x992

- ▶ Authentication (password/login)
- ▶ Smart cards
- ▶ Wireless Personal Area Networking (WPAN)
- ▶ Banking use for money transactions
- ▶ Dormant encryption functionality



5x992

Mass Market Encryption

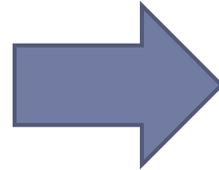
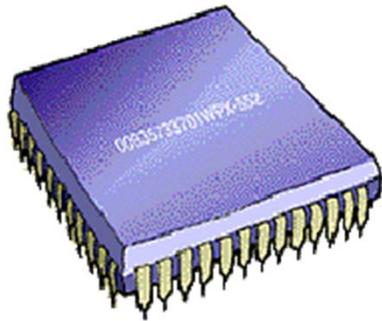
- ▶ Available for purchase (online, telephone, over the counter)
- ▶ Cost
- ▶ Target market



Mass Market ENCRYPTION items get favorable treatment under 5x992



Components of mmr items



Mass Market

5x992

- ▶ “Cryptography Note” (Note 3 to Cat. 5, Part 2)
- ▶ AT controls only (licenses for E:I countries)
- ▶ >64 bit symmetric/ >768 asym/ > 128 ellp. curve

742.15 Sub¶	Item Description	End Users	Submission Requirements
(b)(1)	Items that meet Note 3 of Cat. 5 Part 2 (>64 bit)	All except E1	1. Encryption Registration ERN (Supp. 5 to Part 742) 2. Annual Self-Classification Report (Supp. 8, Part 742)
(b)(3)	Note 3, and (i) Encryption components (chips, electronic assemblies, crypto libraries, toolkit, dev kits) (ii) Non-standard crypto items	All except E1	1. Encryption Registration ERN (Supp. 5 to Part 742) 2. Classification req. with 30 day wait (Supp. 6, Part 742) CCATS
(b)(4)	Note 3, and (i) Short-range Wireless	All except E1	None



Laptops

- ▶ What is on the laptop?
 - ▶ Software/ hardware/ technology
- ▶ How are the items classified?
 - ▶ Windows OSs are 5D992 mass market
- ▶ Where is the laptop going?
- ▶ What license exceptions are available to use?



5x002

- ▶ NS/EI/AT Controlled
 - ▶ >56/512/112-bit* symmetric/asymmetric/elliptic encryption (5A002)
 - *excluding items using only limited cryptographic functionality as defined in the related control note
 - ▶ Also other things like cryptanalytic gear
 - ▶ Need authorization to export
 - use a license exception, if applicable
 - ▶ If no License exceptions apply, then a license is required!
-



ENC

- ▶ (a)(1) –development/production by private end user HQ'd in Supp. 3
- ▶ (a)(2) –Any internal purpose by U.S. Subs
- ▶ (b)(1)- all items except described in b2 and b3 to everywhere
- ▶ (b)(2) – gov't end users outside Supp. 3
 - ▶ (b)(2)(i)-(iv) - network infrastructure, encryption source code quantum cryptography, penetration testing, public safety radio (P25/Tetra), OCl, cryptanalytic, encryption technology (5E002)
- ▶ (b)(3) -
 - ▶ (b)(3)(i) – components, chips, crypto libraries, toolkits, dev kits
 - ▶ (b)(3)(ii) – “non-standard cryptography”
 - ▶ (b)(3)(iii) – digital forensics



ENC/MMR Requirement Matrix

	Encryption Registration	Annual Self-Classification Report	30 day review	Semi-Annual Reporting
ENC A				
ENC B1	X	X		
ENC B2	X		X	X
ENC B3	X		X	B3iii
ENC B4				
MMR B1	X	X		
MMR B3	X		X	
MMR B4				



Things to file

- ▶ **Encryption Registration:** (748.3(d), 740.17(d))
 - ▶ Supplement 5 to Part 742– submit in SNAP-R.
 - ▶ Exporter will receive an **ERN** (encryption registration number, R#) in SNAP-R.
- ▶ **Annual Self Classification Report:** (742.15 (c))
 - ▶ Supplement 8 to Part 742
 - ▶ send via email to BIS and NSA
- ▶ **Encryption Classification Request:** (740.17 (d)), 748.3 (d))
 - ▶ Supplement 6 to Part 742 (encryption questionnaire) - submit in SNAP-R
 - ▶ **CCATS = G# issued by BIS**
- ▶ **Semi-Annual Reporting Requirement:** (740.17 (e))



License required

- ▶ Export to E:I countries
- ▶ (b)(2) controlled items → Government end users outside Supp. 3
- ▶ Cryptanalytic → any government end user
- ▶ Non-standard/cryptanalytic technology and OCI → any end user that is not in or HQed in Supp. 3
- ▶ Encryption Technology (5E002) → end users in DI (unless HQed in Supp. 3) and gov't outside Supp. 3

The future

- ▶ Cat. 4 and Cat. 5 part I new controls – cyber products

