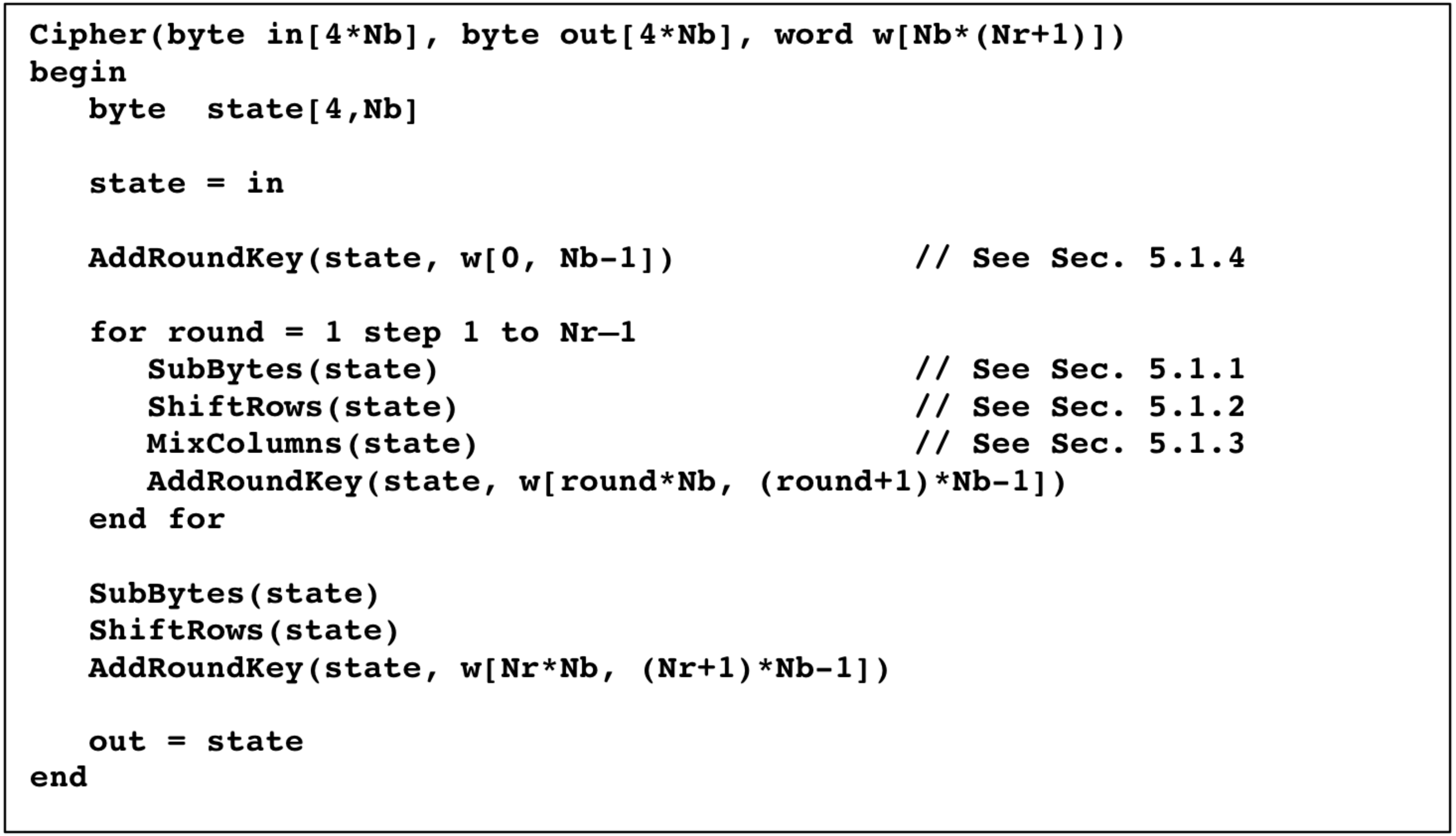
Kevin M. Stoffell
CISSP-ISSAP, ISSEP, ISSMP, CISA, CEH, CAP, PMP, CSEP
Battelle Memorial Institute
ISC2 Authorized Instructor

Level-Setting Security Training Material for the Security Professional Dynamically



```
Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
   byte  state[4,Nb]

   state = in

   AddRoundKey(state, w[0, Nb-1])            // See Sec. 5.1.4

   for round = 1 step 1 to Nr–1
      SubBytes(state)                        // See Sec. 5.1.1
      ShiftRows(state)                       // See Sec. 5.1.2
      MixColumns(state)                      // See Sec. 5.1.3
      AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
   end for

   SubBytes(state)
   ShiftRows(state)
   AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])

   out = state
end
```

Problems to Address

- Problem: Maintenance of multiple sets of training material for different audience types

- Problem: Loss of student focus/engagement if material is not set to the appropriate level of detail/complexity for the audience.

Training Material Modularization by Design

- Deliberate process
  - Identify audiences
  - Identify Learning Objectives (LO) for each audience
  - Plan time budget
  - Allocate LO's to delivery formats
  - Develop material and delivery plan
  - Pilot material with intended audiences and adjust
  - Monitor and update over time

Dynamic Level Setting techniques

- Learn your audience
- Budget extra time/variable use time
- Incorporate multi-use examples / anecdotes
    - Use recurring example themes
- Maximize diagram/graphic based material
- Anticipate and prepare for audience interest areas
    - Practice, practice practice
    - "Murder Boards"
- Pre-planned material deviations
    - Don't be afraid to go off-slide

Adapting existing material

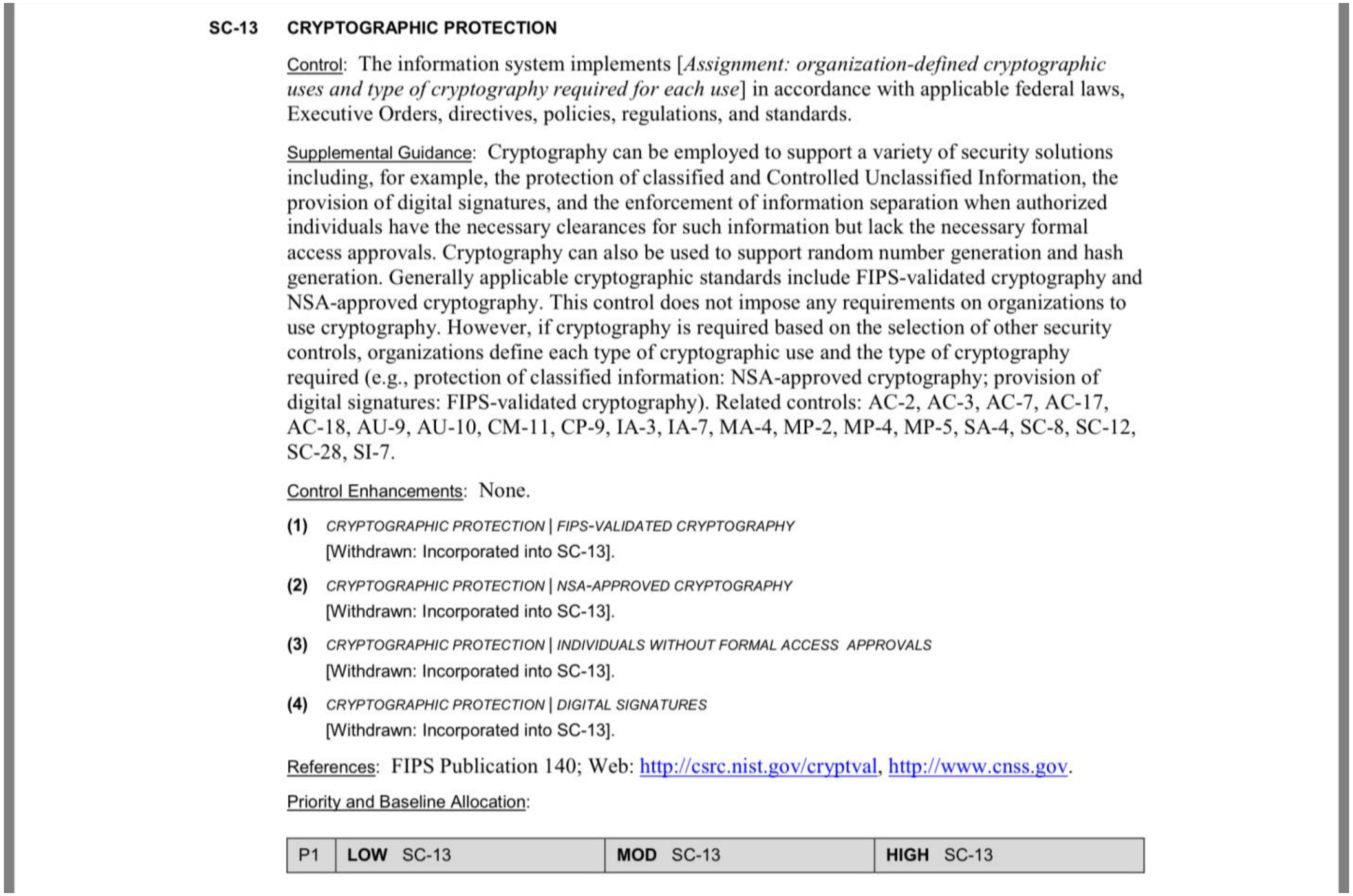
- Utilize surveys
- Identify gaps/recurring questions
- Adjust time budget to free variable use time
- Map new LO's to material

Grow it organically!

Example-Scenario

- Training package on NIST SP 800-53 requirements
- Multiple audiences and levels of technical knowledge
- Significant variance in LO's between potential audiences
- Significant interest level variance
- Example constrained to NIST resources

Example-SP 800-53, SC-13



SC-13 CRYPTOGRAPHIC PROTECTION

Control: The information system implements [*Assignment: organization-defined cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Supplemental Guidance: Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information: NSA-approved cryptography; provision of digital signatures: FIPS-validated cryptography). Related controls: AC-2, AC-3, AC-7, AC-17, AC-18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7.

Control Enhancements: None.

(1) *CRYPTOGRAPHIC PROTECTION | FIPS-VALIDATED CRYPTOGRAPHY*
[Withdrawn: Incorporated into SC-13].

(2) *CRYPTOGRAPHIC PROTECTION | NSA-APPROVED CRYPTOGRAPHY*
[Withdrawn: Incorporated into SC-13].

(3) *CRYPTOGRAPHIC PROTECTION | INDIVIDUALS WITHOUT FORMAL ACCESS APPROVALS*
[Withdrawn: Incorporated into SC-13].

(4) *CRYPTOGRAPHIC PROTECTION | DIGITAL SIGNATURES*
[Withdrawn: Incorporated into SC-13].

References: FIPS Publication 140; Web: http://csrc.nist.gov/cryptval, http://www.cnss.gov.

Priority and Baseline Allocation:

P1	**LOW** SC-13	**MOD** SC-13	**HIGH** SC-13

Example-Requirements SC-13

Audience	Learning Objective	Format	Budget
Manager/PM	Existence/Mandatory	Summary slide	1 min
Crypto User	Why / value	Summary slide	30 sec
C&A Staff	Applicability (Evaluation)	Specific slide (External)	2 min 2 min
Capability Manager	Mandatory conditions Applicability	Specific slide Generic diagram	2 min 2 min
Tester / assessor	Evaluation	External	5 min
System Admin	Operation (Evaluation)	Specific slide (External)	1 min 2 min
ISSE	Implementation	Specific slide Generic diagram External	3 min 5 min 7 min
Developer	Design constraints	Specific slide External	2 min 3 min
Architect	Integration Interoperability	Specific slide Generic diagram	1 min 4 min

Example-Summary slide

- Other info
- Other info
- Cryptography standards
- Other info
- Other info

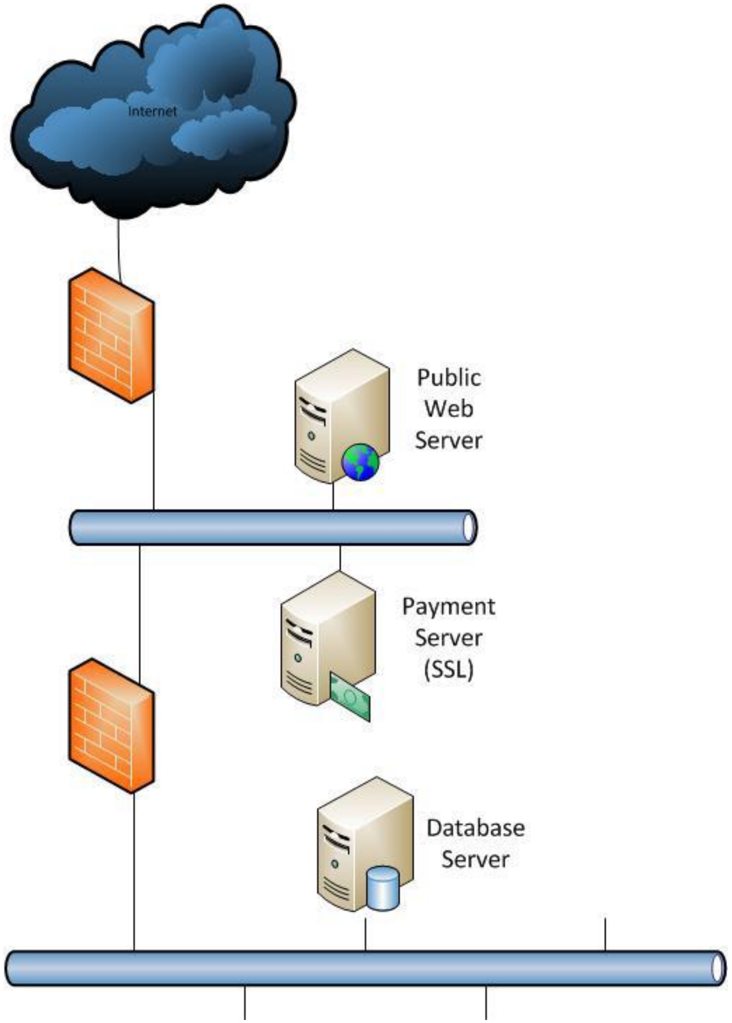
Example-SC-13 specific slide

- Algorithms
  - CAVP
- Federal Information Processing Standards 140-2
  - Applicability
  - CMVP
  - Levels
- Common Applications
- Implementation issues
- http://csrc.nist.gov/projects/crypto.html

Example-Eval External

- FIPS 140-2 source
- SP 800-53 source
- SP 800-53A source
- Live/recorded CAVP website
- Live/recorded CMVP website
- Selected certificates/evaluation reports

Example-Generic diagram



Questions?

Stoffellk@battelle.org

Battelle

The Business *of* Innovation