THALES

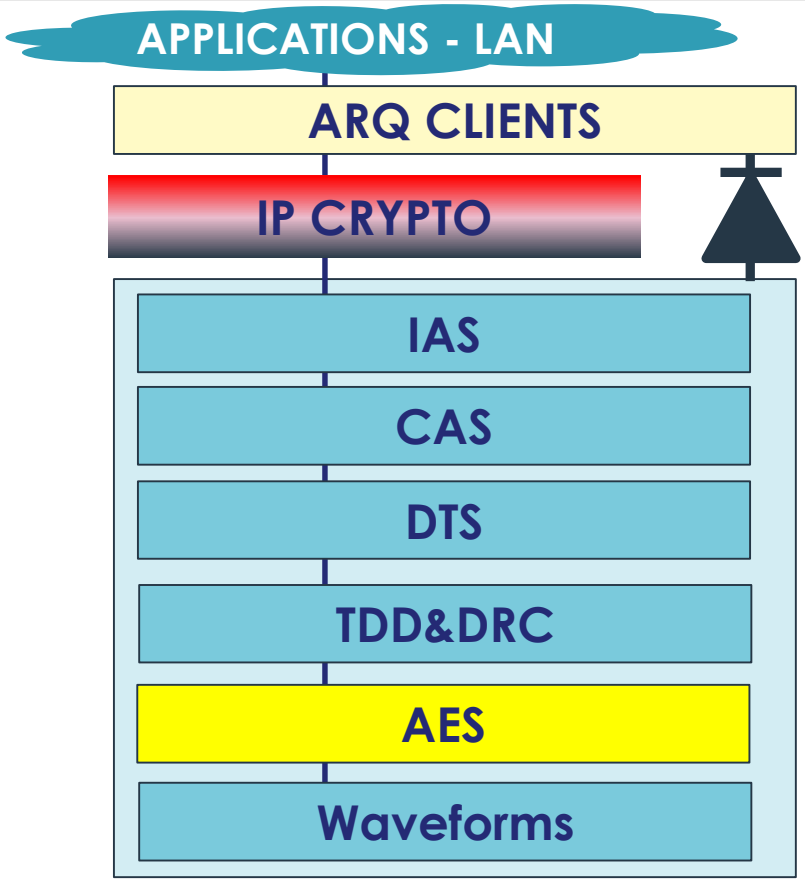
AES in STANAG 5070 Protection of protocol elements

NATO BLOS, Stockholm. 15 August 2019
Sue Trinder, Philippe Crambert, Jean-Luc Rogier, Rodolphe Kuhn

Agenda

- Generic presentation of AES
- Application to protection of protocol elements in STANAG 5070
- Status update on ST5070 annexes

STANAG 5070 architecture - reminder



ARQ server &modem

OPEN

Protection of information

Information	Protected by
Operational information	IP crypto
User's IP addresses	IP crypto
IP crypto red address	N/A: not transmitted over the air
IP crypto black address	STANAG 5070 AES
DSCP	STANAG 5070 AES
ARQ protocol elements: ARQ addresses, PDU Type, TX frame seq number, Time To Die	STANAG 5070 AES
ALE protocol elements : ALE addresses	Sodark as in MIL-STD-188-141

Ops data are protected by the IP crypto
Protocol elements are protected by ST5070 AES

What is AES: Advanced Encryption Standard

- **AES is specified by NIST SP800-38A ; was created in 2001**
  - NIST= National Institute of Standards and Technology, reports to the US Chamber of commerce
- **AES is widely used, eg by HTTPS**
- **Several open sources implementations are available, some are even evaluated by the NIST (eg open SSL used by HTTPS)**
- **Vendors can also decide to implement their own version as the AES algorithm is public**
- **AES uses**
  - secret keys
  - And an Initialisation Vector, or counter depending on node, that can be public
- **AES mandates that 2 transmissions are not done with the same (key + IV)**

Modes in AES

AES actually contains several modes

- Some bring integrity on top of confidentiality: not needed for ST5070 as there is already an ARQ
- Some propagate transmission errors: not a good idea for HF

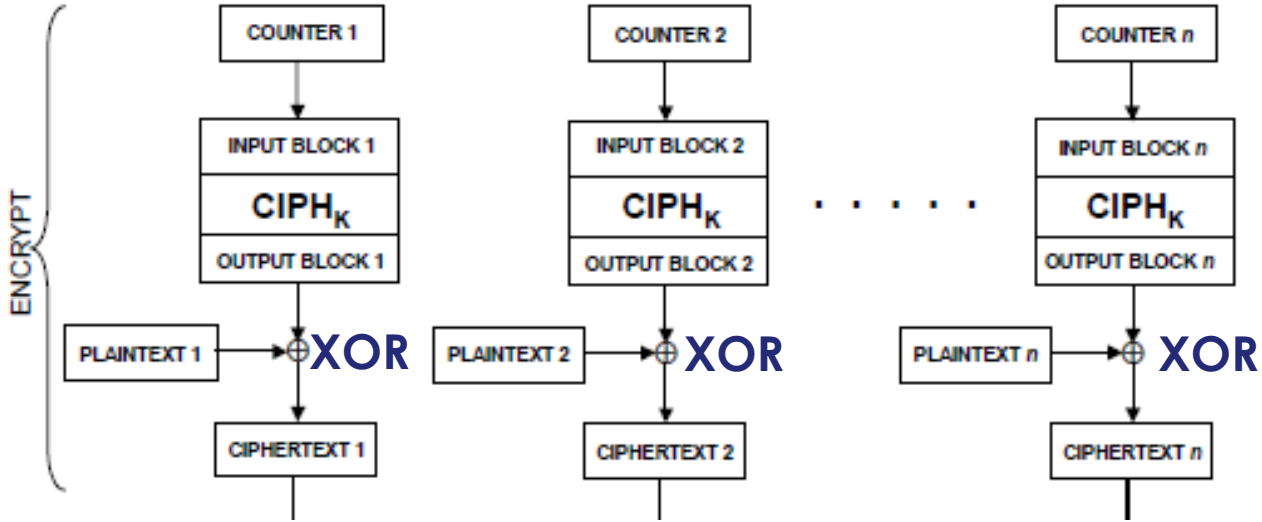
The best candidate for HF is the COUNTER MODE (CTR), as described in §6.5 of NIST SP800-38A

It is based on 128 bit blocks produced from a counter and ciphered via the key

These 128 bit blocks are then Xored with the plain text

The CTR mode in AES

All blocks are128 bits



Consequences:

- **No propagation of error**
- **No overhead of ciphering on a packet per packet basis** (but transmission of keys and counter to be discussed in next slides

Agenda

- Generic presentation of AES
- Application to protection of protocol elements in STANAG 5070
- Status update on ST5070 annexes

Reminder

For the rest of this presentation, please remember that use of AES in STANAG 5070 is to protect protocol elements, not to protect operational information (which is already protected by an IP crypto)

Discussion on keys

128 or 256 bit keys?

- 128 enough today but 256 will be needed when quantum computers exist
- Choice has no significant impact on processing time (14 "rounds" vs 10)

=> **256 bit key recommended; should 128 bits be considered as an option for potential export control restrictions?**

Keys have to remain secret

- To avoid OTA overhead, keys will be distributed manually (fill guns or modern equivalent eg USB key)
- A practical system will avoid operators to have to load keys into the system too often; it will be better if keys can be used for a long time
- To avoid erosion of the key, the same (key + counter) is not to be used twice; as keys are to be used for a long time, this constraint falls therefore upon the counter
- Good news: the counter can be public: it can be generated by a node and communicated to others just before the transmission

Proposed counter structure (numbers TBC)

SECTION 1: 64 bits	SECTION 2: 48 bits	SECTION 3: 16 bits
ALE caller to generate a random sequence before link set-up	TX to generate a random sequence for each TDD slot	Increment +1 for each 128 bit block
Transmitted at link set-up	Transmitted at start of TDD slot	Not transmitted
Valid for all ondes involved in link	Each node generates its own before TX	Computed by TX and RX nodes
Overhead impact can be neglected (64 bits vs an ALE session of potentially several minutes / 10s of minutes)	Overhead discussed in next slide	Not transmitted OTA => no overhead
Let's check if this limits the quantity of data that can be transmitted:	At 800 bps and 1.5s TDD : enables 800x1.5x 2^{48} = 337 770 TERAbits per ALE session…. sufficient for HF for the time being ☺ ☺	Enables 128x 2^{16} = 8.3 Mbits per TDD slot; much more than needed ☺ ☺

128 bits total, only 48 transmitted regularly

THALES

Counter overhead

- Counter to be protected by Reed Solomon 9/16 as errors on counter will cause loss of entire TDD; overhead due to the 48 bits is therefore:

	TDD 1.5s	TDD 9s	NINE crypto
	48 bits per TDD	48 bits per TDD	53 bytes per IP packet; assume MTU 1500 bytes
at 800 bps	7,11%	1,19%	3,53%
at 1200 bps	4,74%	0,79%	3,53%
at 2400 bps	2,37%	0,40%	3,53%
at 4800 bps	1,19%	0,20%	3,53%
at 9600 bps	0,59%	0,10%	2,93%
at 30 000 bps	0,19%	0,03%	3,53%
at 64 000 bps	0,09%	0,01%	3,53%

- ST5070 AES overhead quickly negligible vs IP Crypto; At low rates, longer TDD preferred
- Note that for B'cast modes, counter will be repeated at intervals to enable Late Trafic Entry (LTE)

Summary of protection of protocol elements with STANAG 5070 AES

Benefits	
Keys distributed manually; no OTA overhead; long duration of keys	✓
All protocol elements ciphered	✓
No overhead at IP packet level; limited 48*16/9= 85 bits overhead at each TDD ie every 1.5s or every 9s	✓
Applicable to all waveforms, non-contiguous (ST4539-H) and contiguous (ST 5069)	✓
Applicable to point to point, point to multipoint and B'cast (LTE)	✓
Reuse of open source or vendor own implementation both possible	✓

Agenda

- Generic presentation of AES
- Application to protection of protocol elements in STANAG 5070
- **Status update on ST5070 annexes**

ST5070 updates: v0.4

Volume	Contents	V0.4
Main	Overall presentation	Update posted onto web site early August 2019 Comments received from NOR have been taken into account … and a lot of improvements has been done
Annex A	ALE, ALM	
Annex B	DRC + TDD	
Annex C	ARQ-Red	
Annex D	ARQ-Black	
Annex E	IP crypto	
Annex F	5066 clients	
Annex G (new)	AES	In progress; not released yet
Annex H (new)	IP PEP	In progress; not released yet

FRA MOD posted draft 0.4 of ST5070 onto BLOS web site in early August 2019
Comments just received from NCIA to be addressed in 0.5

THANK YOU FOR YOUR ATTENTION