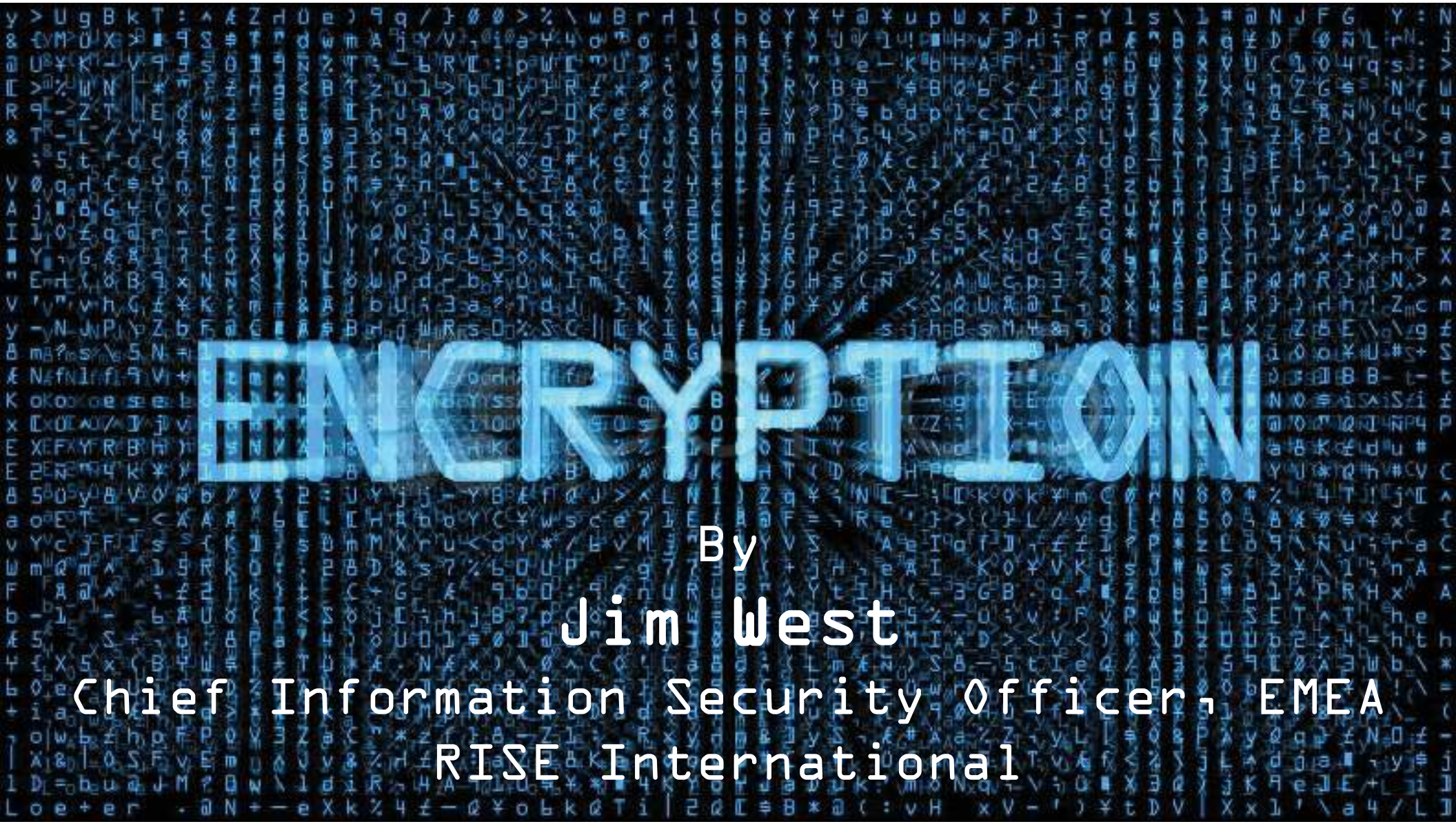
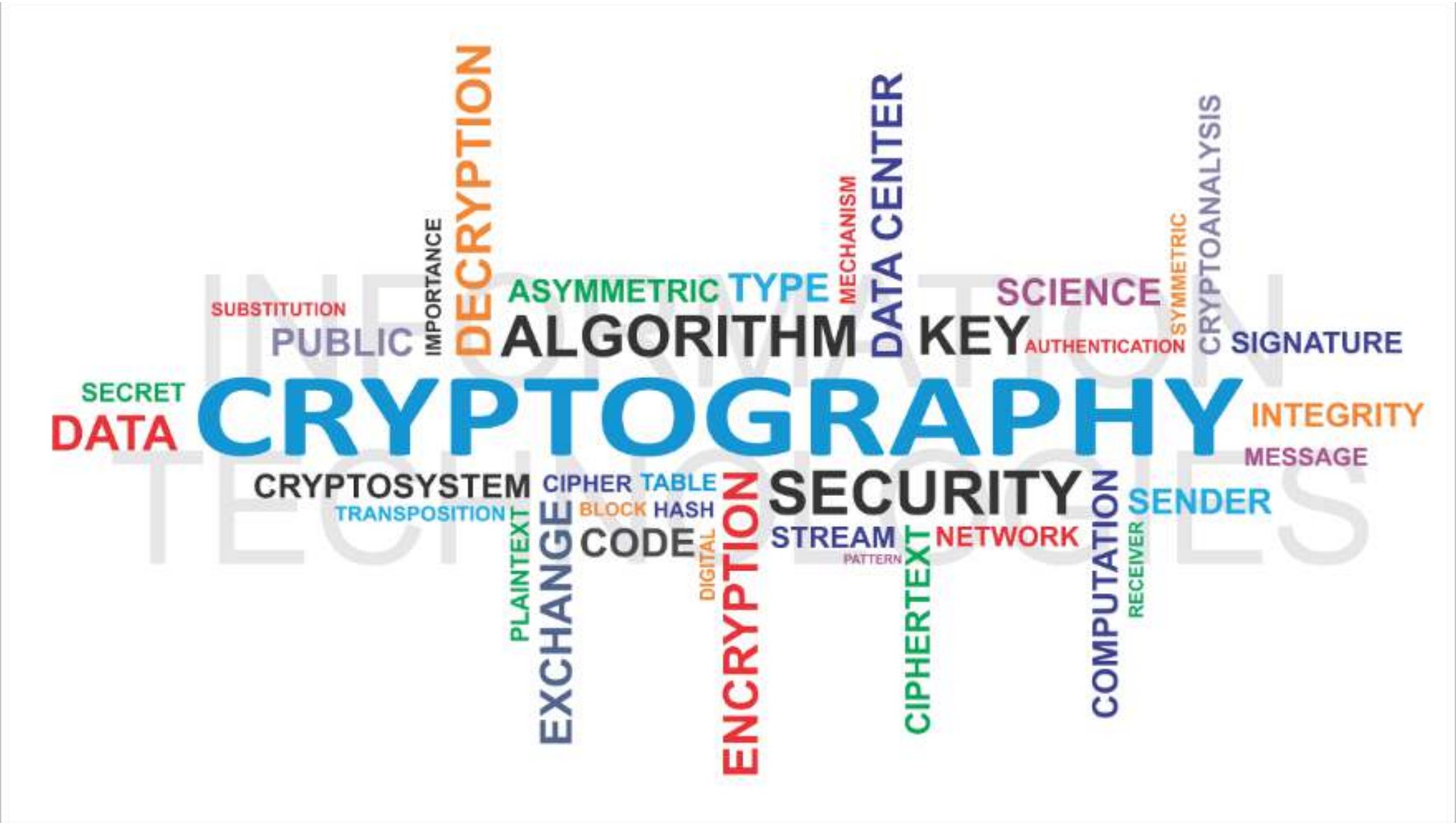
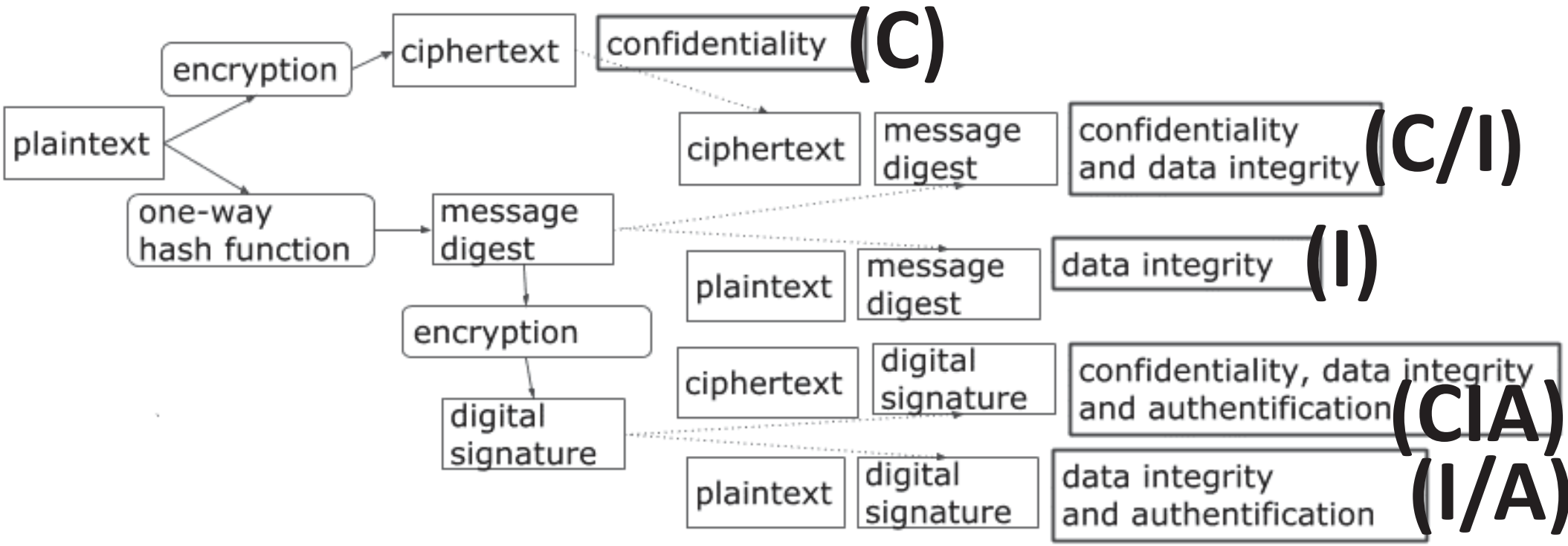

ENCRYPTION
By
Jim West
Chief Information Security Officer, EMEA
RISE International


CRYPTOGRAPHY
SECRET
DATA
PUBLIC
SUBSTITUTION
IMPORTANCE
DECRYPTION
ASYMMETRIC
TYPE
ALGORITHM
MECHANISM
DATA CENTER
KEY
SCIENCE
AUTHENTICATION
SYMMETRIC
CRYPTOANALYSIS
SIGNATURE
INTEGRITY
MESSAGE
CRYPTOSYSTEM
CIPHER
TABLE
TRANSPOSITION
BLOCK
HASH
PLAINTEXT
EXCHANGE
CODE
DIGITAL
ENCRYPTION
SECURITY
STREAM
PATTERN
CIPHERTEXT
NETWORK
SENDER
COMPUTATION
RECEIVER

WHAT IS IT ALL ABOUT?

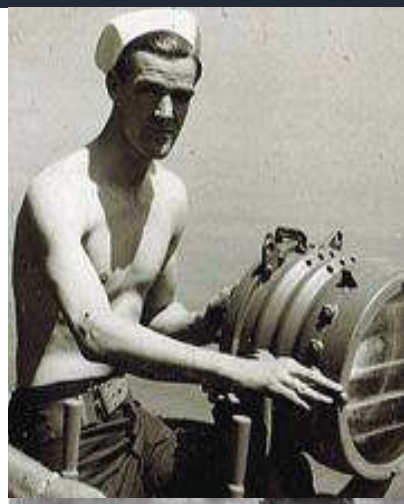
One of the main methods of providing computer networks security is encryption. With billions of financial transactions conducted daily over the Internet, cryptography has become more important than ever. The diagram below shows the overview of the Internet cryptography.



BRIEF HISTORY

MORSE CODE

A ●−	J ●−−−	S ●●●
B −●●●	K −●−	T −
C −●−●	L ●−●●	U ●●−
D −●●	M −−	V ●●●−
E ●	N −●	W ●−−
F ●●−●	O −−−	X −●●−
G −−●	P ●−−●	Y −●−−
H ●●●●	Q −−●−	Z −−●●
I ●●	R ●−●	



BRIEF HISTORY

Navajo Code Talkers' Dictionary

REVISED AS OF 15 JUNE 1945, DECLASSIFIED

Source: Department of the Navy, Naval Historical Center

WORD	NAVAJO WORD	LITERAL TRANSLATION
Corps	DIN-NEH-IH	Clan
Battalion	TACHEENE	Red Soil
Squad	DEBEH-LI-ZINI	Black Sheep
Commanding General	BIH-KEH-HE	War Chief
Colonel	ATSAH-BESH-LE-GAI	Silver Eagle
Dive Bomber	GINI	Chicken Hawk
Observer Plane	NE-AS-JAH	Owl
Fighter Plane	DA-HE-TIH-HI	Humming Bird
Battleship	LO-TSO	Whale
Concentration	TA-LA-HI-JIH	One Place
Halt	TA-AKWAI-I	Halt
Hostile	A-NAH-NE-DZIN	Not Friendly
Mine	HA-GADE	Mine
Navy	TAL-KAH-SILAGO	Sea Soldier
Ordnance	LEI-AZ-JAH	Under Ground
Radar	ESAT-TSANH	Listen
Scout	HA-A-SID-AL-SIZI-GIH	Short Racoon
Tank	CHAY-DA-GAHI	Tortoise

BRIEF HISTORY

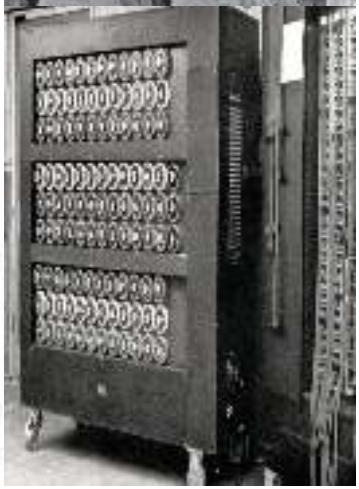
Geheime Kommandosache! Jeder einzelne Tagesschlüssel ist geheim! Mitnahme ins Flugzeug verboten!

Nr. 000082

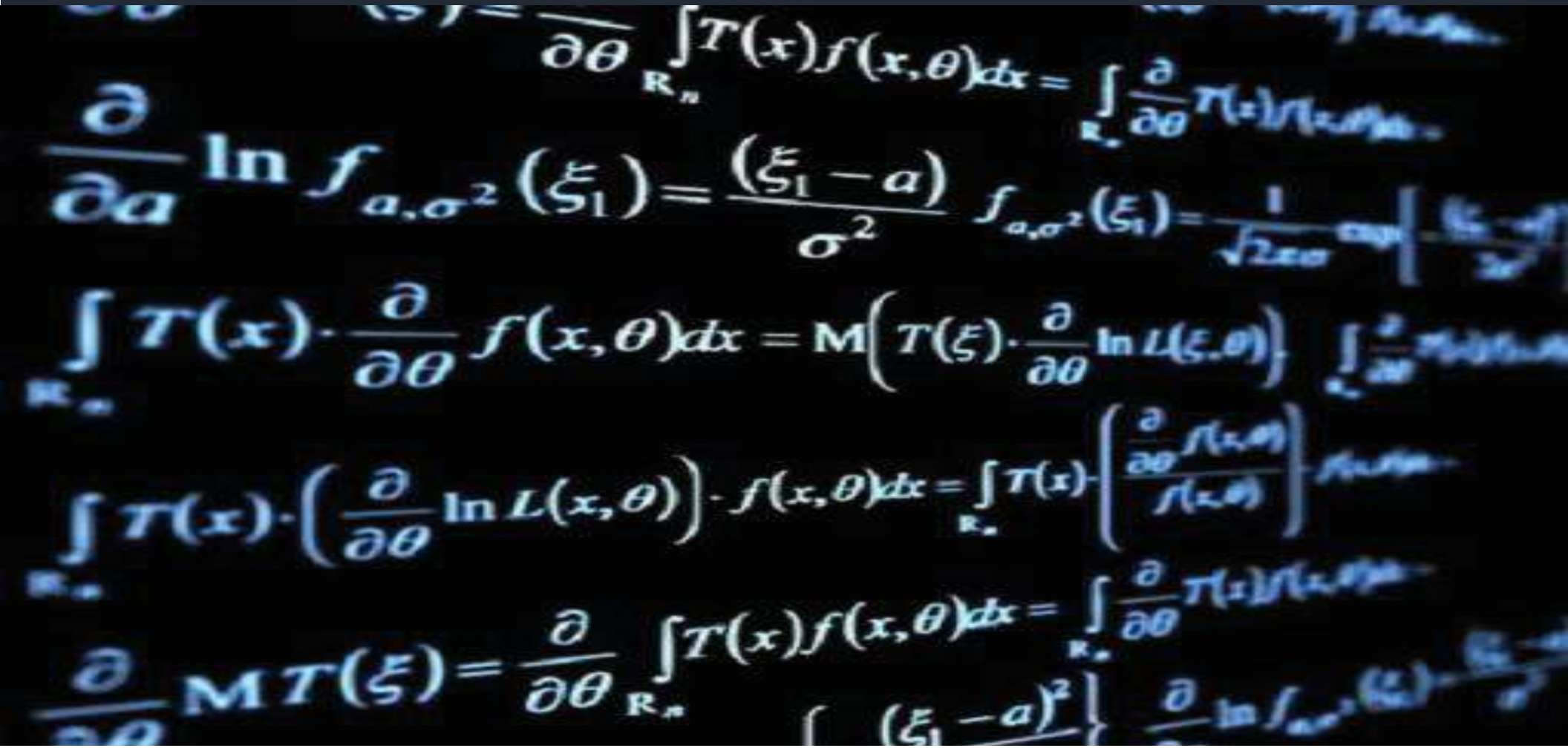
Luftwaffen-Maschinen-Schlüssel Nr. 2744

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und frühzeitig vernichten.

Tag	Walzenlage			Ringstellung			Steckerverbindungen										Zusatzstecker-verbindungen		Kenngruppen			
2744	31	III	V	IV	17	11	04	PA	IM		TW	BI	UY	GP	CK	JQ	DL	RV	EM	AH	NS	FO	kim	pwh	sbx	csw
2744	30	I	IV	V	08	17	21	DI	MF		LS	DH	MT	EO	AF	UZ	FQ	NY	BK	GR	GI	JN	uaq	omn	ume	duf
2744	29	V	II	III	11	14	05	SV	CO		DO	JW	CN	IV	PZ	BM	HU	AL	FR	KX	EQ	GT	don	cqc	xum	bpg
2744	28	II	IV	V	02	20	16	KQ	BP		NT	HK	BW	EP	LQ	AU	OY	PJ	CX	GI	DZ	MR	lui	pyg	sby	dtq
2744	27	III	V	IV	18	13	22	GL	AD	HK	HM	GV	KZ	AI	DQ	NR	ES	BL	OU	FT	CF	JY	cmy	fqr	sci	bur
2744	26	I	III	II	24	10	01	BN	EH	BW	GW	AQ	MO	FY	PS	DI	RU	JZ	BN	EH	KT	CL	kbj	jaq	udm	cns
2744	25	IV	I	III	04	25	23	CM			LT	DR	QX	AG	IN	EU	BJ	KF	FW	CM	SS	HO	kqx	yar	vdb	com
2744	24	V	III	I	09	19	06	BO			GL	MY	CR	SN	JX	DT	AF	PU	IQ	BO	EW	KS	cmz	aoj	zod	auh
2744	23	IV	I	V	15	03	19	EW			IT	DV	HQ	AJ	MU	EX	KG	CS	PY	LN	HP	GZ	kra	yas	xun	cob
2744	22	I	V	III	12	26	07	QV			NY	JL	AK	NV	PZ	OT	HP	MX	BQ	OS	DW	IO	jdm	uhf	xuo	bph
2744	21	III	IV	II	15	09	12				JP	DY	QS	HL	AE	NW	CU	IK	PX	BR	MV	GO	jpf	aok	iys	btx
2744	20	IV	II	I	02	22	05				HY	NP	AM	DX	GJ	KQ	BS	OV	BR	CW	IU	FL	boy	wac	uow	cse
2744	19	V	I	II	06	19	17				GM	OX	BY	QU	DP	HJ	PK	SW	AN	EL	CY	IR	xjc	wad	unj	rtd
2744	18	III	IV	I	11	21	01				KW	IP	DM	SV	JR	CX	EN	AZ	QT	BU	PH	GY	xpn	rzi	vcm	bpo
2744	17	I	V	II	18	23	14				BV	HW	AR	NI	DS	PT	CZ	PI	LY	EJ	GK	MQ	kdx	crq	vcn	cod
2744	16	III	IV	V	16	04	07				LU	CV	FN	KR	BY	GH	QW	DJ	PS	AO	EI	HX	lgx	jri	uob	aur
2744	15	V	III	IV	24	13	10				HZ	NQ	AD	TV	IX	EM	BG	LO	CE	RY	JU	FP	wpi	vhy	zoe	aus
2744	14	I	IV	II	05	30	25				FN	UY	CJ	IW	LP	AS	DK	GQ	MO	BZ	BT	MR	wog	hxi	xxi	bpi
2744	13	III	II	I	03	26	18				KR	IZ	AT	NV	EH	MF	CO	OY	ES	DP	UW	LQ	iqv	iqb	zay	coe
2744	12	II	IV	III	04	11	15	AG	BG		DT	JV	HS	CI	AY	KU	EN	FQ	LR	BW	MP	GO	zic	myt	zof	dtr
2744	11	V	I	IV	16	07	02	IA	FV		JS	PW	AV	QX	DN	IZ	KM	CO	EG	PL	HY	BR	inf	xbm	krz	dug
2744	10	IV	III	II	20	12	14	BH	RU		PS	CQ	JO	PR	AW	HV	EZ	KN	DU	OT	IL	BT	ink	acu	zxj	cnu
2744	9	III	II	V	06	18	10	GS	QX		BK	TZ	MX	LW	GQ	AD	NY	BE	CS	JP	RV	IO	efm	pmi	znw	cof
2744	8	V	I	III	01	21	17	DZ	PA		GU	SW	BP	KZ	EV	OT	LQ	CH	IP	KY	JM	NZ	imy	rjw	tjm	cog
2744	7	II	V	I	25	08	23	NV	EI	AG	CX	AS	DV	KY	HU	LW	GP	EY	MR	FQ	IN	OS	inv	rkc	znx	bpj
2744	6	IV	II	V	13	26	03	BG	FW	EI	DV	LP	NQ	QZ	OS	PK	EW	MR	IT	HX	UY	BJ	yvu	hab	swq	aut
2744	5	III	I	II	24	19	22	FV	PA	QX	SY	EK	NZ	OX	CG	JM	QU	PV	BI	LW	TX	DP	seu	iqe	swr	suv
2744	4	II	IV	I	17	05	09	RU	QX	PA	BD	GV	AX	KP	EM	FN	CW	RU	HO	JT	IL	QS	xfj	hxj	zxk	dpt
2744	3	V	II	IV	20	16	11	HL	KN	FW	JT	NW	DU	EO	XV	BY	PS	HQ	IM	LX	GP	CR	clx	zbn	zxa	buk
2744	2	II	III	V	14	03	19	DS	OW	PA	RW	OQ	GI	AZ	BJ	MS	CU	DH	PY	BF	LV	TX	ljs	jro	spq	coh
2744	1	III	I	IV	18	24	15				NP	JV	LY	IX	HQ	AO	DZ	CR	FZ	EM	GS	SW	pif	dgw	tjn	cnv



BRIEF HISTORY



CURRENT DoD STANDARDS

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	**Symmetric** block cipher used for information protection	FIPS Pub 197	Use 256 bit keys to protect up to TOP SECRET
Elliptic Curve Diffie-Hellman (ECDH) Key Exchange	***Asymmetric*** algorithm used for key establishment	NIST SP 800-56A	Use Curve P-384 to protect up to TOP SECRET.
Elliptic Curve Digital Signature Algorithm (ECDSA)	***Asymmetric*** algorithm used for digital signatures	FIPS Pub 186-4	Use Curve P-384 to protect up to TOP SECRET.
Secure Hash Algorithm (SHA)	Algorithm used for computing a condensed representation of information	FIPS Pub 180-4	Use SHA-384 to protect up to TOP SECRET.
Diffie-Hellman (DH) Key Exchange	***Asymmetric*** algorithm used for key establishment	IETF RFC 3526	Minimum 3072-bit modulus to protect up to TOP SECRET
RSA	***Asymmetric*** algorithm used for key establishment	NIST SP 800-56B rev 1	Minimum 3072-bit modulus to protect up to TOP SECRET
RSA	***Asymmetric*** algorithm used for digital signatures	FIPS PUB 186-4	Minimum 3072 bit-modulus to protect up to TOP SECRET.

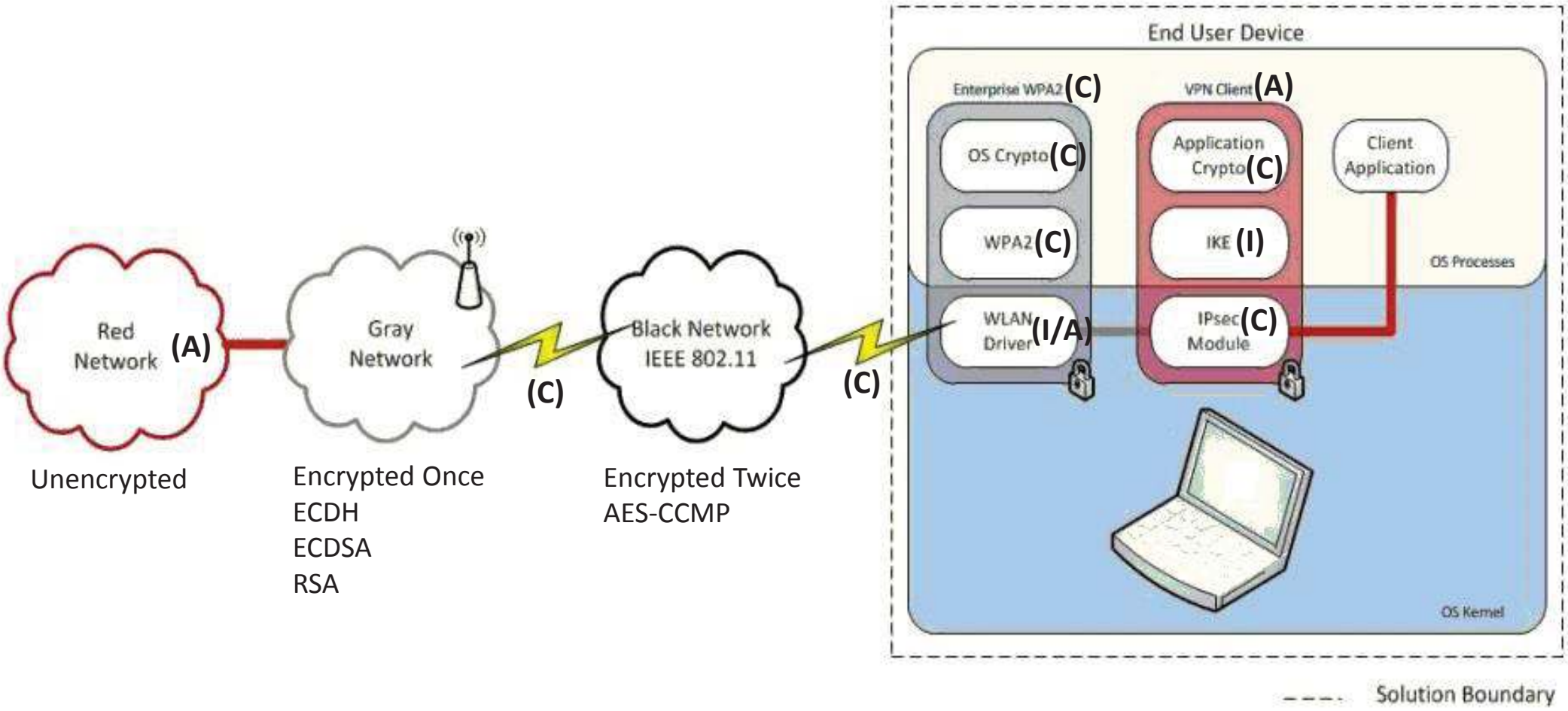
THE FUTURE OF CRYPTO

IAD will **initiate a transition to quantum resistant algorithms in the not too distant future**. Based on experience in deploying Suite B, we have determined to start planning and communicating early about the upcoming transition to quantum resistant algorithms. Our ultimate **goal is to provide cost effective security against a potential quantum computer**. We are working with partners across the USG, vendors, and standards bodies to ensure there is a clear plan for getting a new suite of algorithms that are developed in an open and transparent manner that will form the foundation of our next Suite of cryptographic algorithms.

Until this new suite is developed and products are available implementing the quantum resistant suite, **we will rely on current algorithms.** For those partners and vendors that have not yet made the transition to Suite B elliptic curve algorithms, **we recommend not making a significant expenditure to do so at this point but instead to prepare for the upcoming quantum resistant algorithm transition**.

https://www.nsa.gov/ia/programs/suiteb_cryptography/

CsFC - Commercial Solutions for Class.

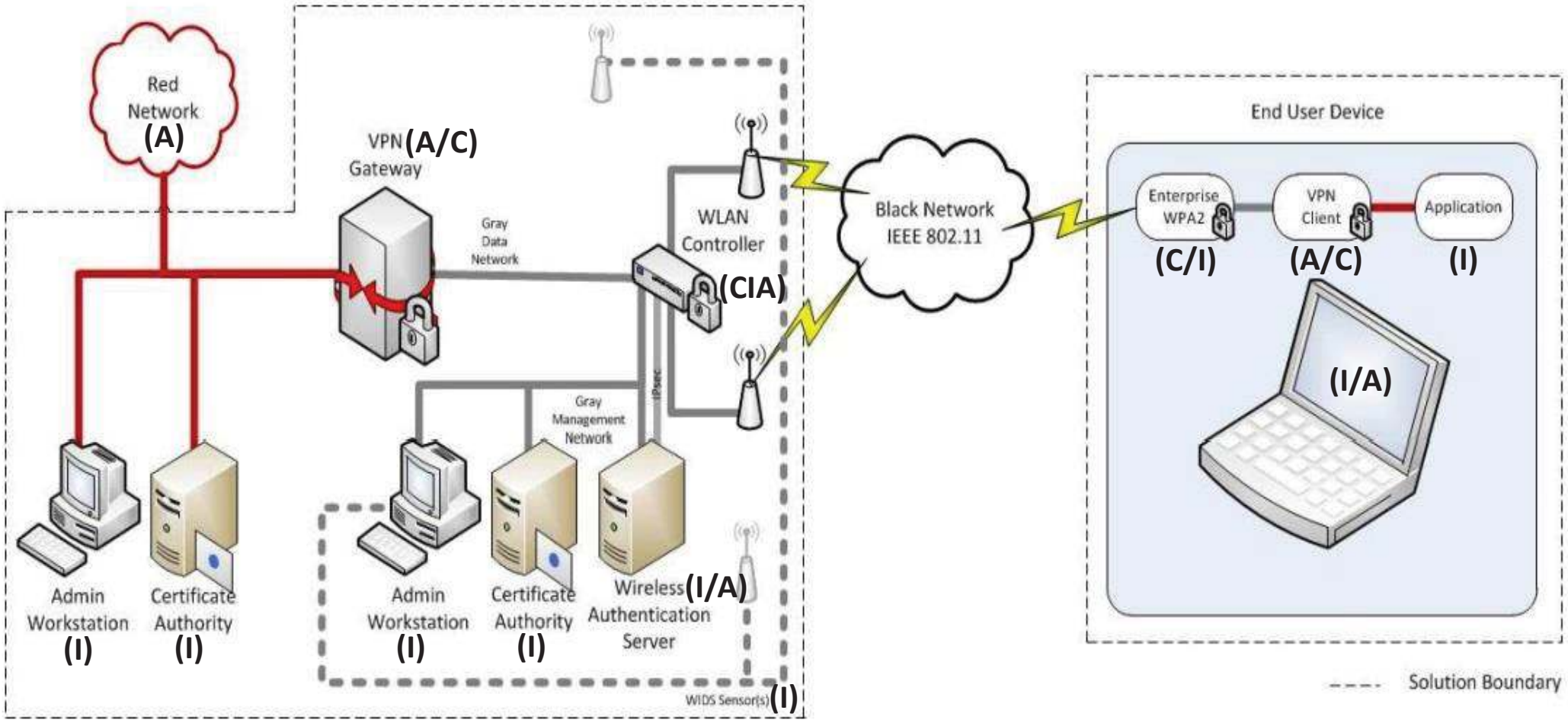


Unencrypted

Encrypted Once
ECDH
ECDSA
RSA

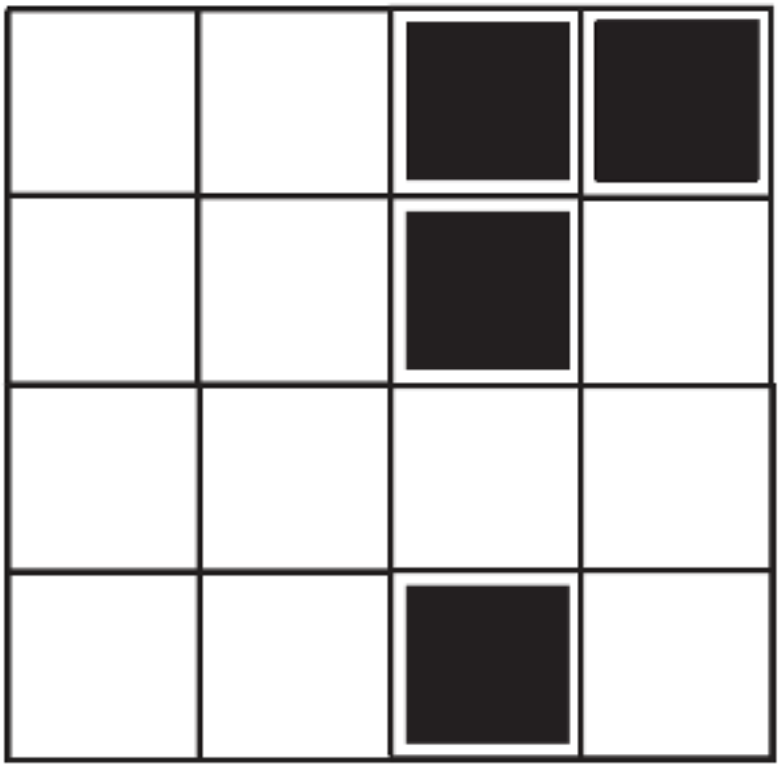
Encrypted Twice
AES-CCMP

CsFC - Commercial Solutions for Class.



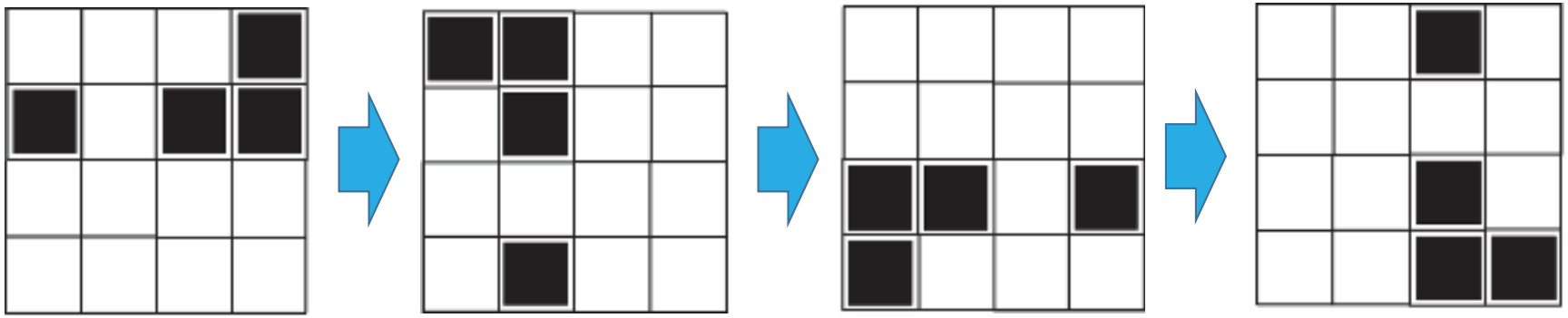

ENCRYPTION
DEMO-1

DEMO 1



C	R	O	U
N	Y	E	N
T	E	R	D
W	P	D	S

SECRET KEY



UNENCRYPTEDWORDS


ENCRYPTION
DEMO-2