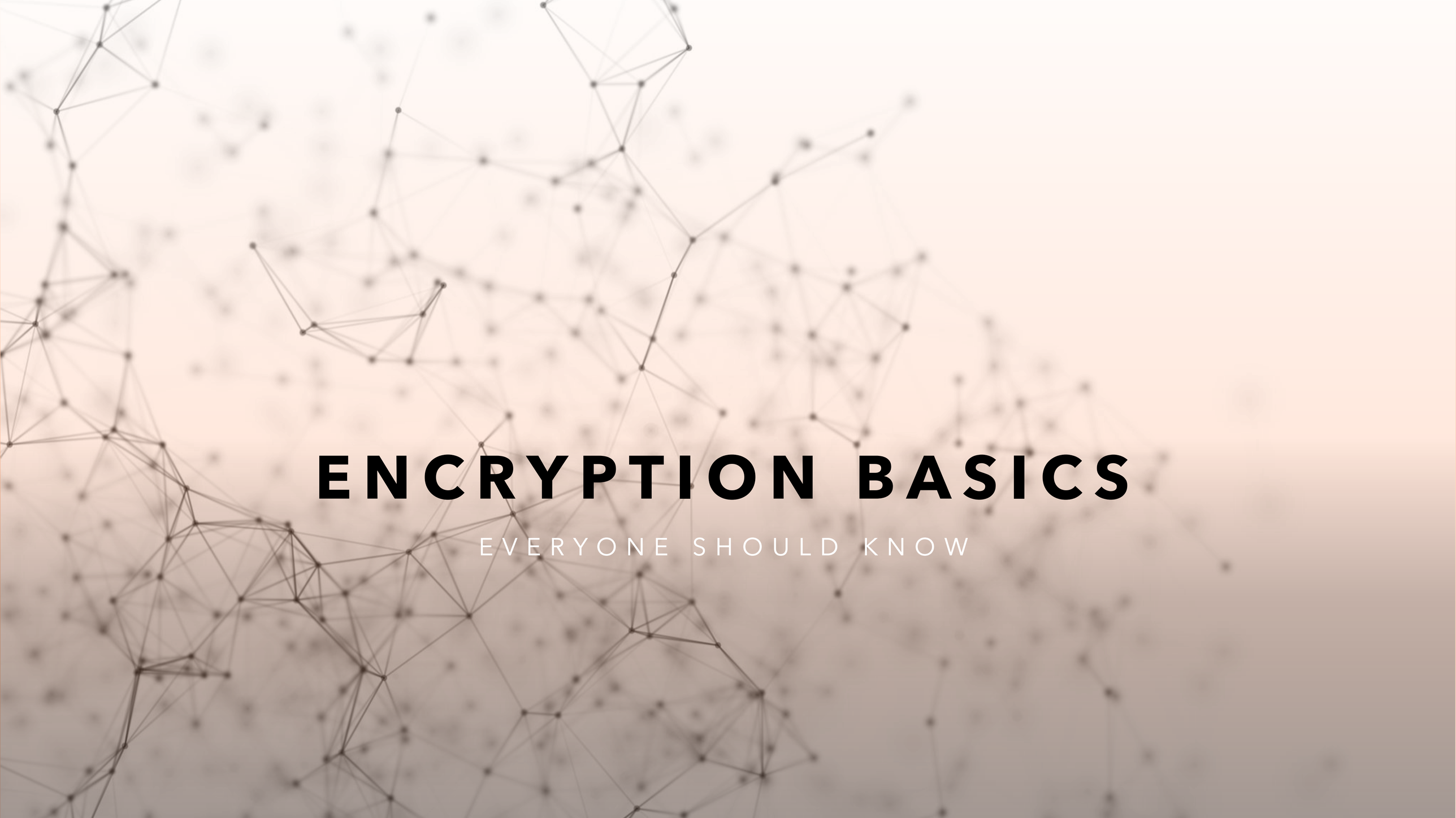
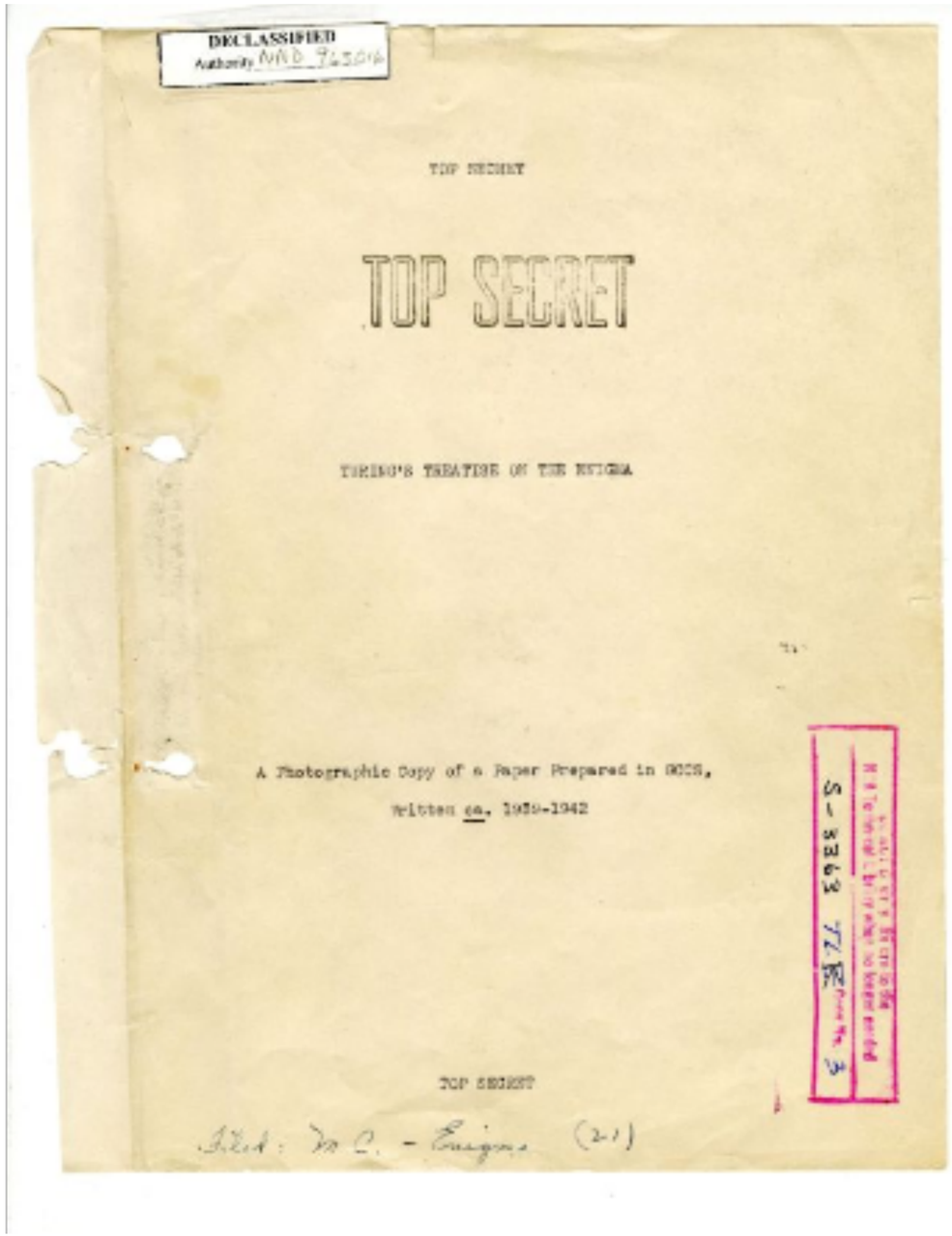

ENCRYPTION BASICS
EVERYONE SHOULD KNOW

FIRST RULE OF CRYPTO:

DON'T ROLL YOUR OWN CRYPTO

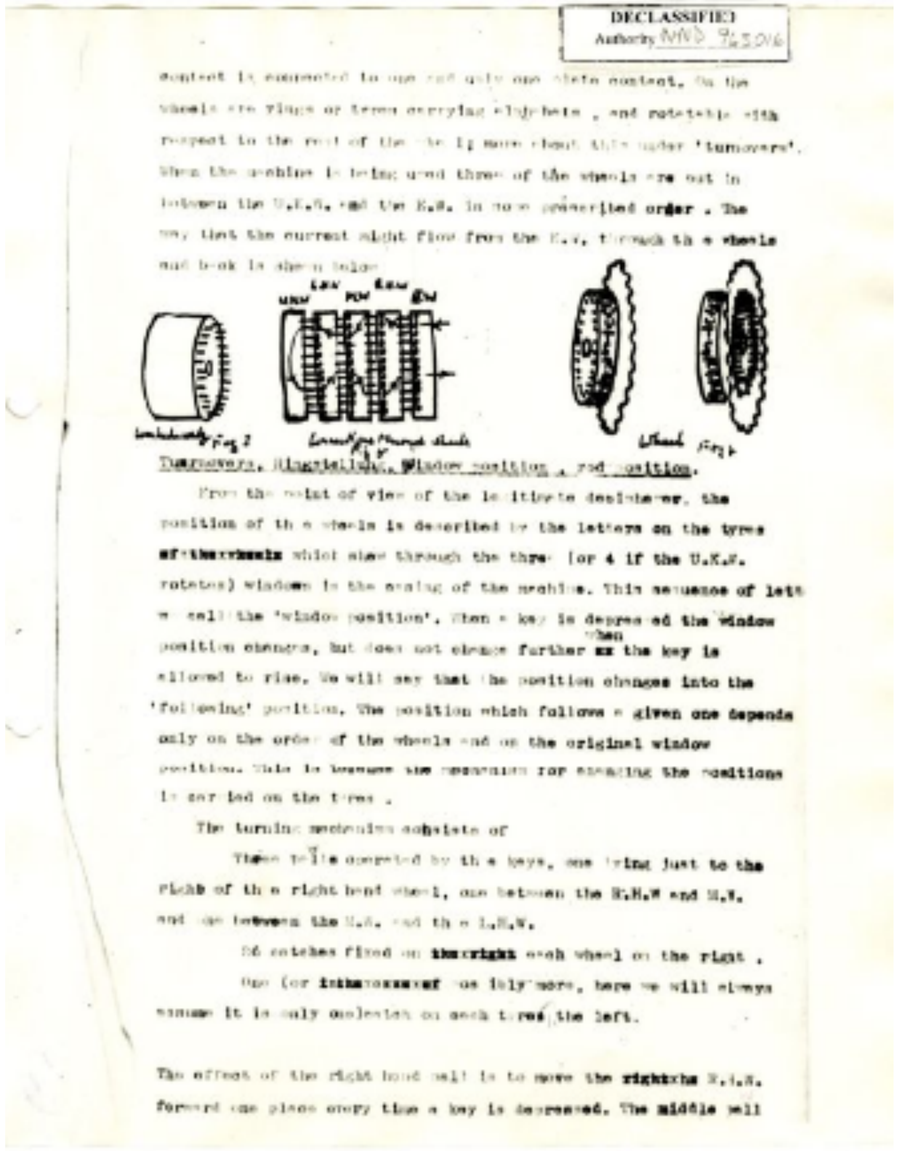


BAD EXAMPLES

- AT&T's Clipper Chip
- BassOmatic
- Telegram's MTProto
- Crown Sterling

ADDITIONAL RULES

- Encryption is not the answer to security
- Cryptography is not easy
- Cryptography is not cheap



DECLASSIFIED
Authority NND 963016

Context is connected to one and only one plate contact. On the wheels are rings or tyres carrying alphabets , and rotatable with respect to the rest of the wheel (more about this under 'turnovers'. When the machine is being used three of the wheels are put in between the U.K.W. and the E.W. in some prescribed order . The way that the current might flow from the E.W. through the wheels and back is shown below.

Turnovers, Ringstellung, Window position , rod position.

From the point of view of the legitimate dealer, the position of the wheels is described by the letters on the tyres of the wheels which show through the three (or 4 if the U.K.W. rotates) windows in the casing of the machine. This sequence of letters will be called the 'window position'. When a key is depressed the window position changes, but does not change further when the key is allowed to rise. We will say that the position changes into the 'following' position. The position which follows a given one depends only on the order of the wheels and on the original window position. This is because the mechanism for changing the positions is carried on the tyres .

The turning mechanism consists of

Three pins operated by the keys, one being just to the right of the right hand wheel, one between the M.H.W and M.W. and one between the M.M. and the L.H.W.

26 catches fixed on the right each wheel on the right .

One (or more, if necessary as will always assume it is only one) each tyre to the left.

The effect of the right hand pin is to move the right hand W.H.W. forward one place every time a key is depressed. The middle pin

THE REALITY

- Algorithms will be broken
- The time from acceptance to deprecation is shrinking
- Be thoughtful how the cryptography is applied to your system

EXTINCTION

- RC2/RC4
- (X)DES
- SHA-1
- MD2/MD4/MD5
- RSA < 1024bits
- ECDSA - 160bits
- SSL

APPLIED CRYPTOGRAPHY

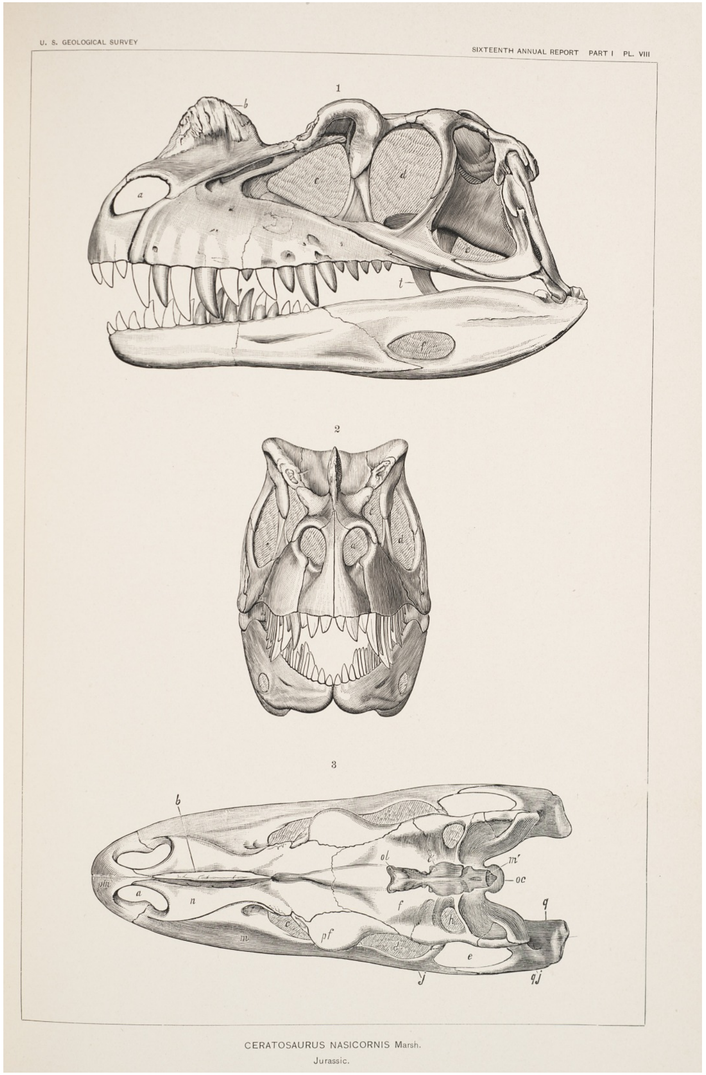
- Symmetric encryption (AES)
- Asymmetric encryption (ElGamal)
- Hybrid (symmetric & asymmetric)
- Public-key cryptography (Wallets, ECC)
- Algorithms
- Random number generation
- Multi-signature
- Multi-party computation
- Encryption in transit (SSL, TLS)
- Encryption at rest
- Digital certificates
- Digital wallets
- Hashes (MD5, SHA)
- Seeds
- Sharding (Shamir’s Secret Sharing)

THE CRYPTO OF CRYPTO

- Random number generators
- Key ceremonies
- Hashing (BTC SHA-256)
- Digital signatures
- Multi-signature
- Multi-party computation
- Mix networks

HOW TO REDUCE RISK

- All device encryption
- VPNs all the time
- Encrypted applications (messaging, voice)
- Multi-signature wallets
- Use applications compatible with TPM
- Physical hardware keys



RESOURCES

- Cryptocurrency Security Standard (CCSS)
- Digital Asset Custody Standard (DACS)
- NIST 800-175B
- NIST FIPS 140-2
- NIST 800-90A

THANK YOU

JASON TRUPPI

@NotTruppi | @Paydropinc