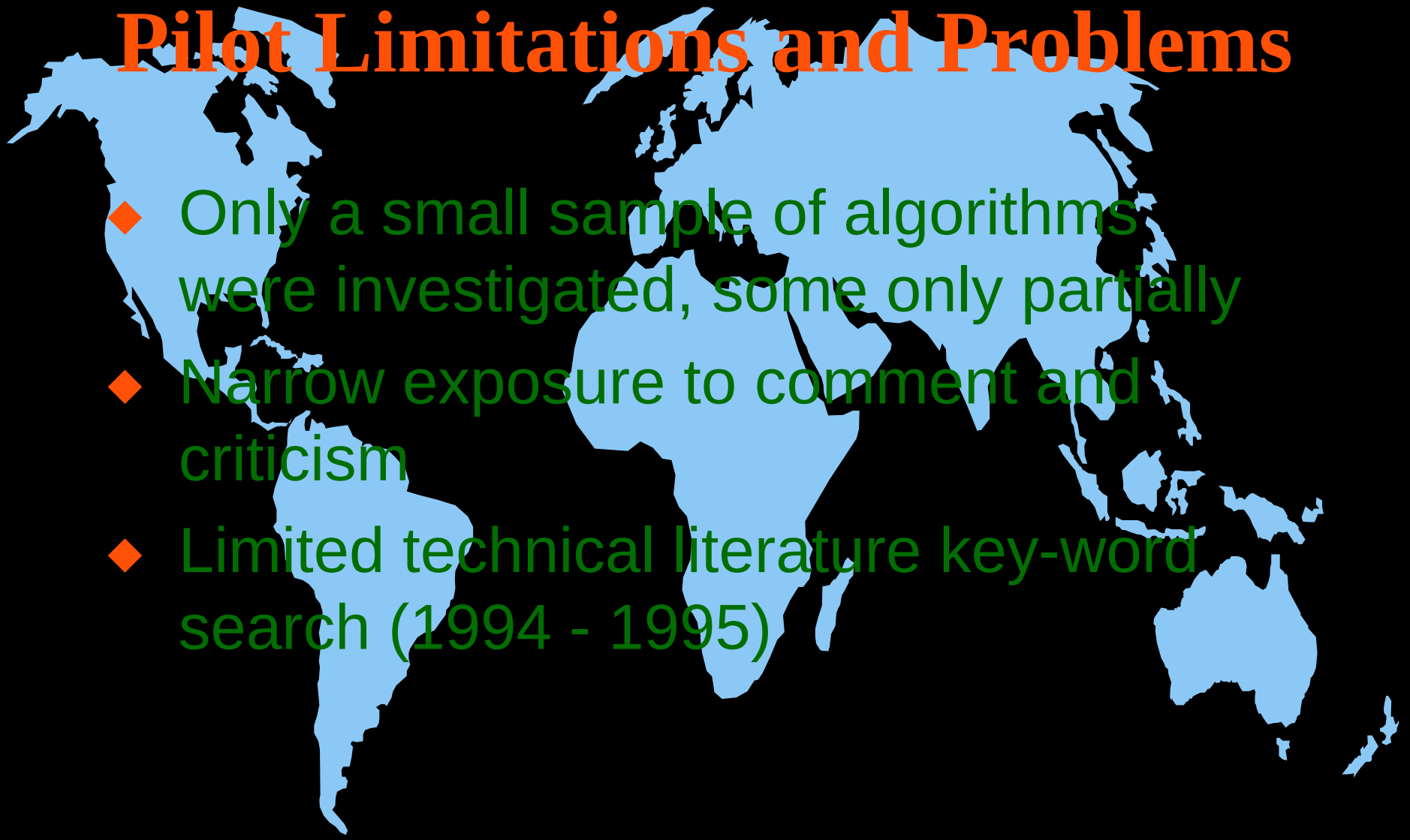
Cryptographic Algorithm Metrics Pilot Investigation

Colonel L[illegible] Smith, J[illegible]
In[illegible] efense[illegible]
[illegible]38-58[illegible]9

Pilot Purposes

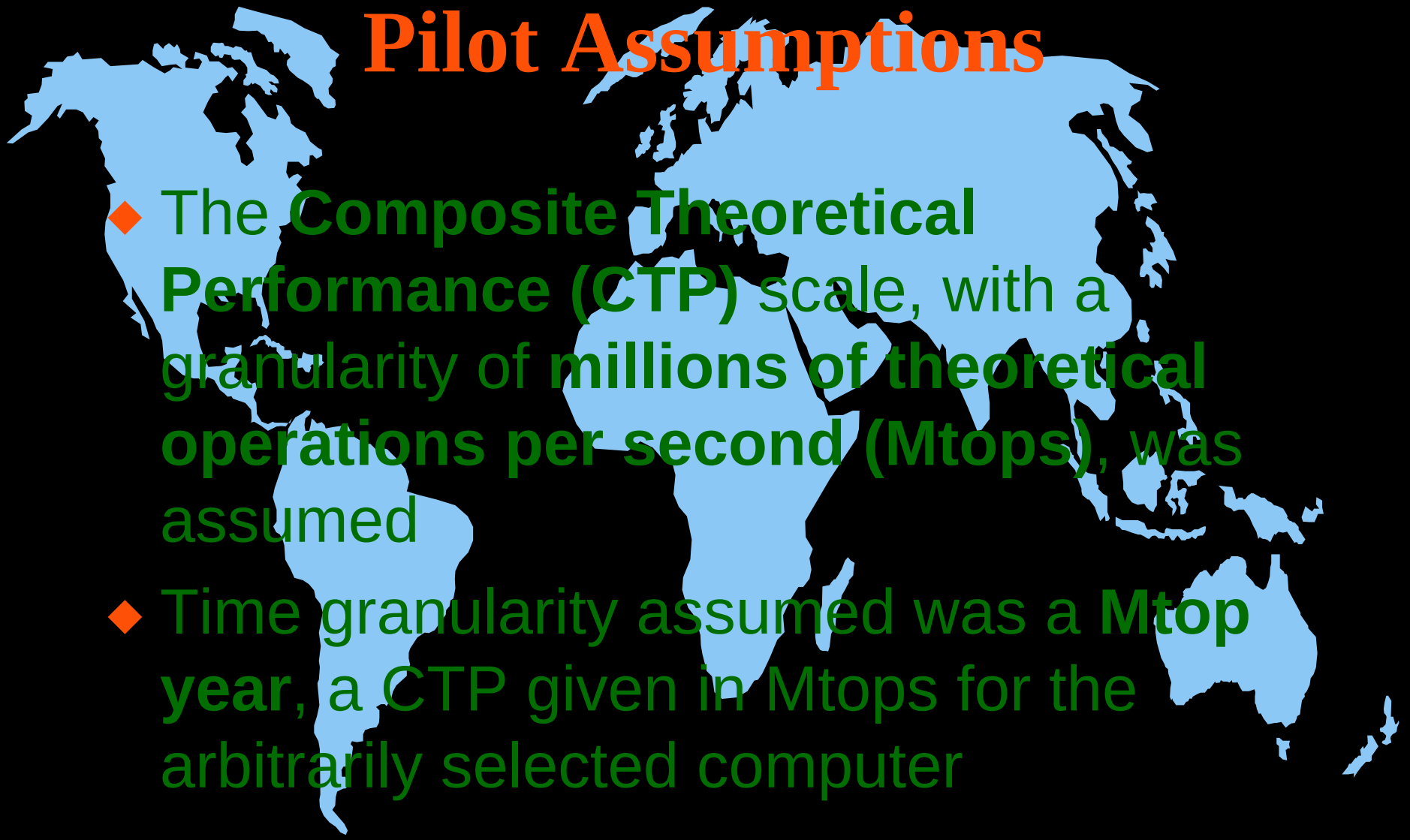
- Explore the possibility of finding:
  - An approach to developing metrics for cryptography
  - Using only public domain sources
- Prompt further investigations
- Evolve into a standard

Pilot Limitations and Problems



- Only a small sample of algorithms were investigated, some only partially
- Narrow exposure to comment and criticism
- Limited technical literature key-word search (1994 - 1995)

Pilot Assumptions

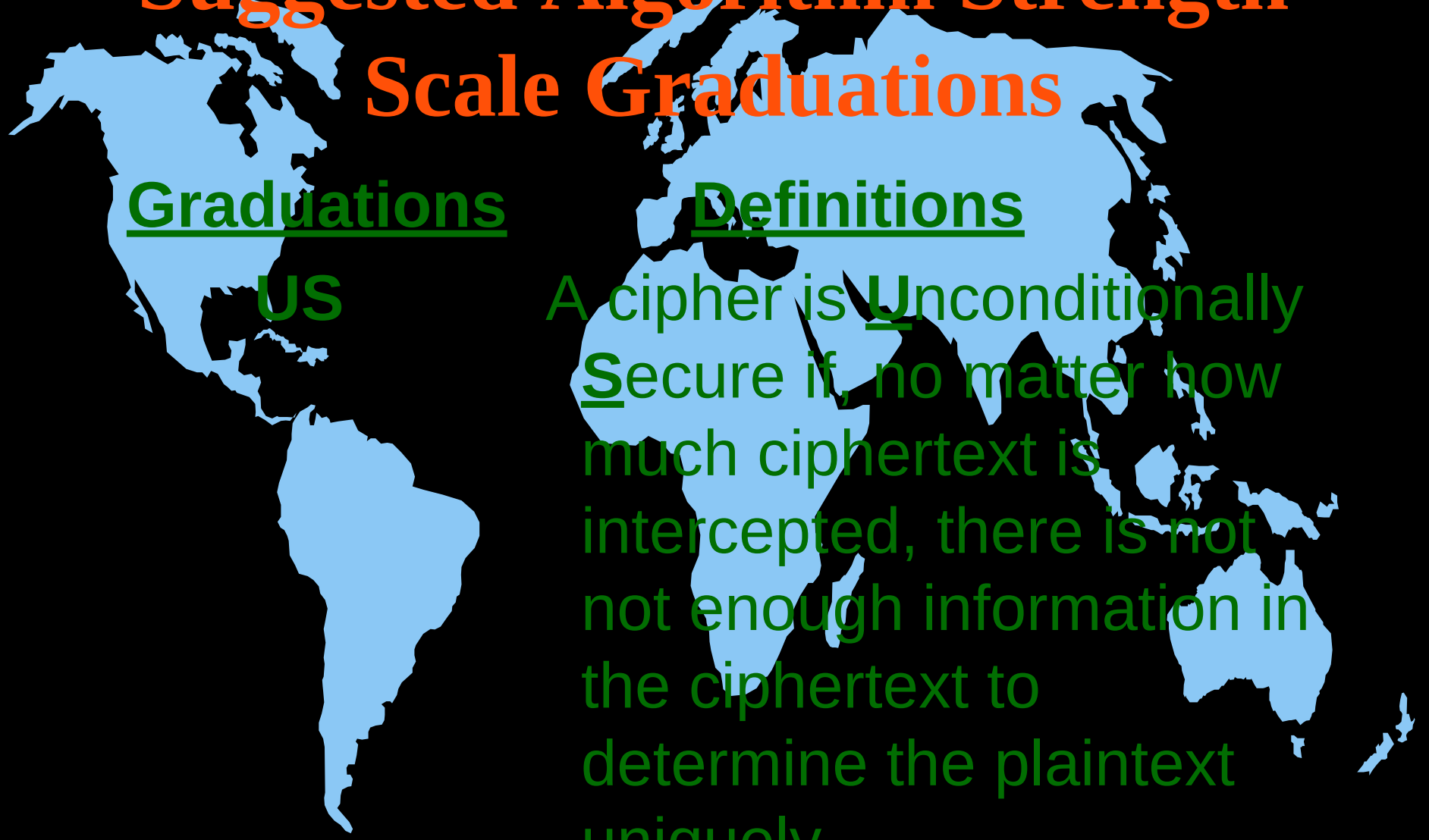


- The **Composite Theoretical Performance (CTP)** scale, with a granularity of **millions of theoretical operations per second (Mtops)**, was assumed
- Time granularity assumed was a **Mtop year**, a CTP given in Mtops for the arbitrarily selected computer

Pilot Assumptions (Continued)

- Attack Time Metric Computer Selection
  - DEC AlphaServer 2100 4/275
  - Symmetrical multiprocessor
  - 1216 Mtops (243,200 MIPs)
  - Reasonably available internationally
  - Affordable ($75K)

Suggested Algorithm Strength Scale Graduations



Graduations	Definitions
US	A cipher is **U**nconditionally **S**ecure if, no matter how much ciphertext is intercepted, there is not not enough information in the ciphertext to determine the plaintext uniquely

Suggested Algorithm Strength Scale Graduations (Continued)

Graduations	Definitions
CS	A cipher is **C**omputationally **S**ecure if it cannot be broken by systematic analysis with available resources in a short enough time to permit exploitation

Suggested Algorithm Strength Scale Graduations (Continued)

Graduations	Definitions
CCS	A cipher is **C**onditionally **C**omputationally **S**ecure if the cipher could be implemented with keys that are not quite “long enough” or with not quite “enough” rounds to warrant a CS rating

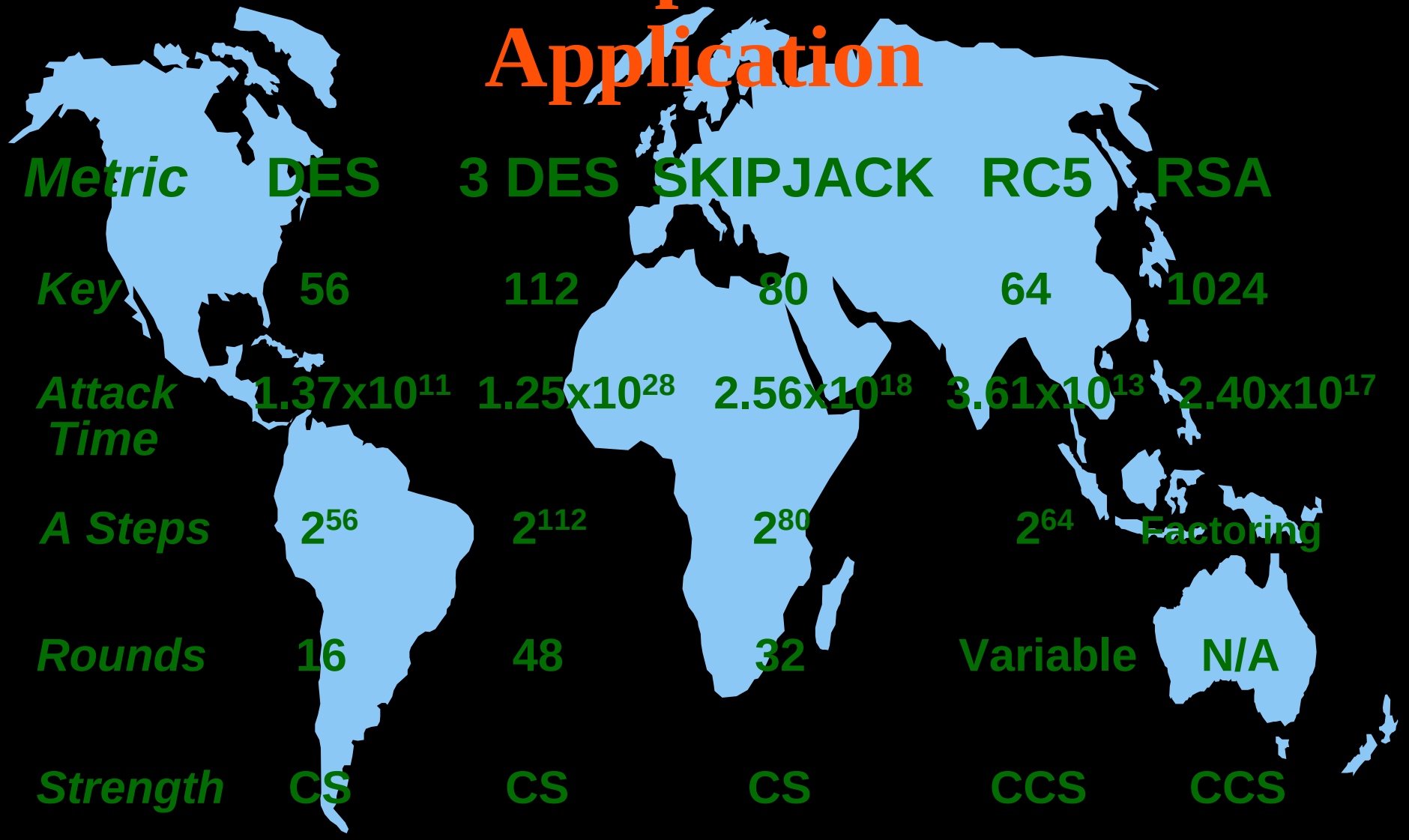
Suggested Algorithm Strength Scale Graduations (Continued)

Graduations	Definitions
W	A Weak cipher can be broken by a brute force attack in an acceptable length of time with an "affordable" investment in cryptanalytic resources (24 hrs & $200K)

Suggested Algorithm Strength Scale Graduations (Continued)

Graduations	Definitions
VW	A Very Weak cipher is one that can be broken by determining the key systematically in a short period of time with a small investment (8 hrs & $20K)

Pilot Example of Metrics Application



Metric	DES	3 DES	SKIPJACK	RC5	RSA
Key	56	112	80	64	1024
Attack Time	1.37×10^{11}	1.25×10^{28}	2.56×10^{18}	3.61×10^{13}	2.40×10^{17}
A Steps	2^{56}	2^{112}	2^{80}	2^{64}	Factoring
Rounds	16	48	32	Variable	N/A
Strength	CS	CS	CS	CCS	CCS

Summary

- It should be possible to develop metrics for the specification of cryptography
- If so, a USG agency (TBR) and (or) The American National Standards Institute should develop a cryptography metrics standard
- Comments, criticisms and recommendations are invited