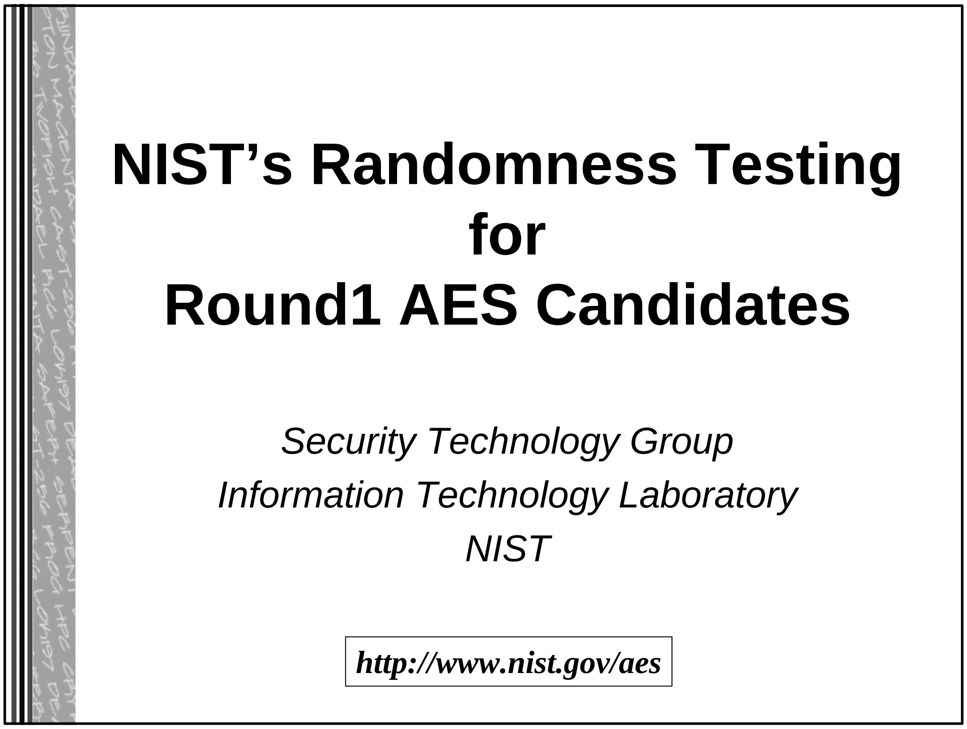
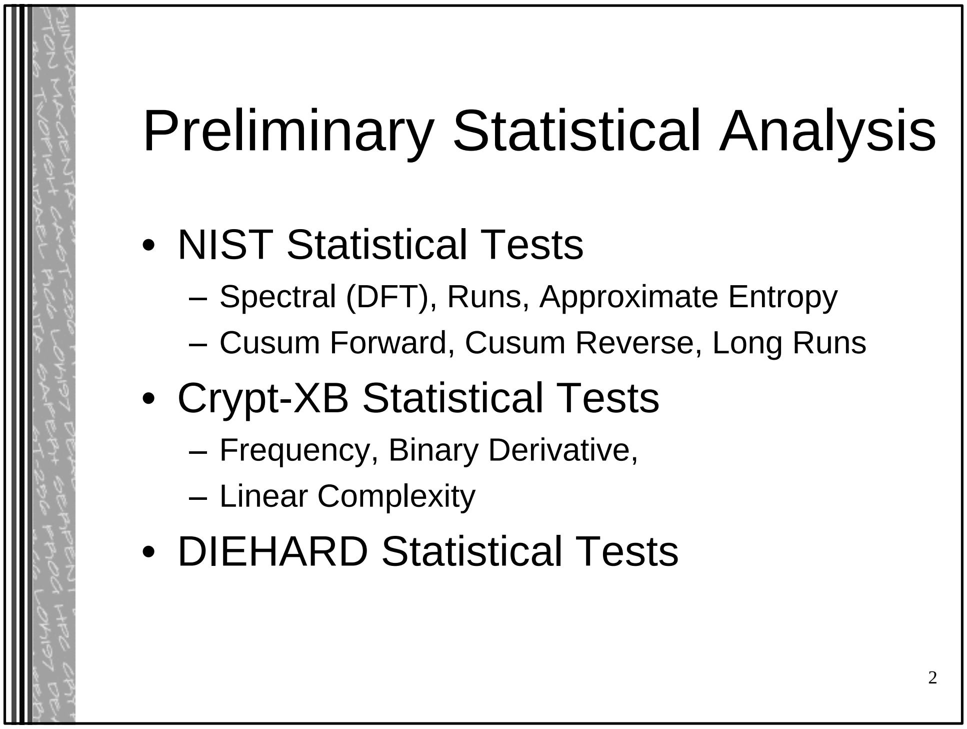


NIST’s Randomness Testing for Round1 AES Candidates

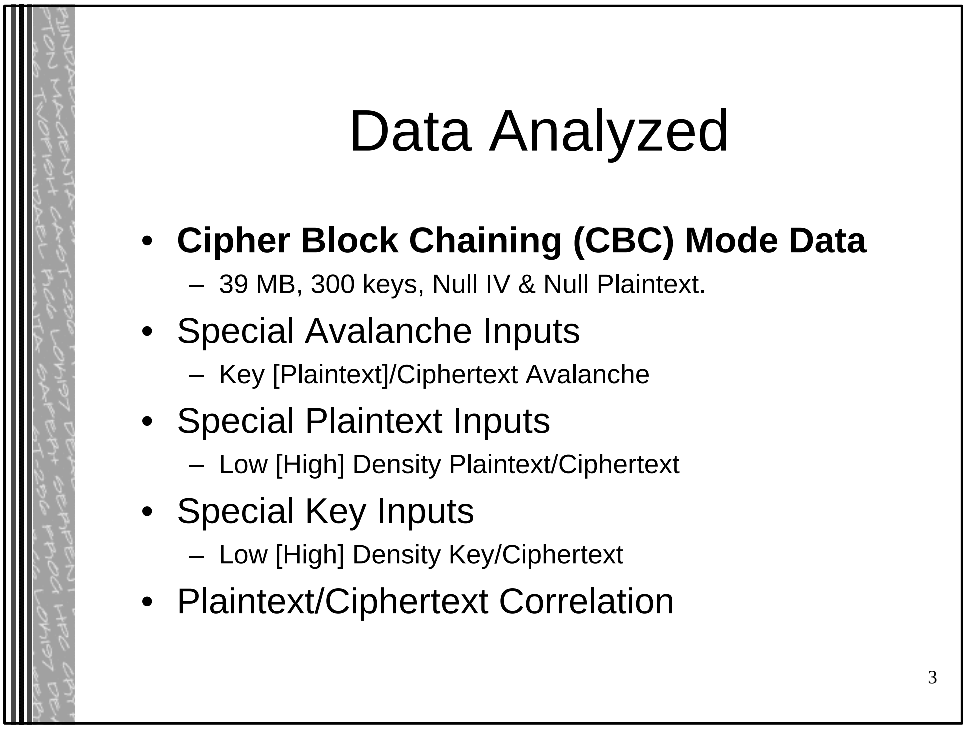
Security Technology Group
Information Technology Laboratory
NIST

http://www.nist.gov/aes



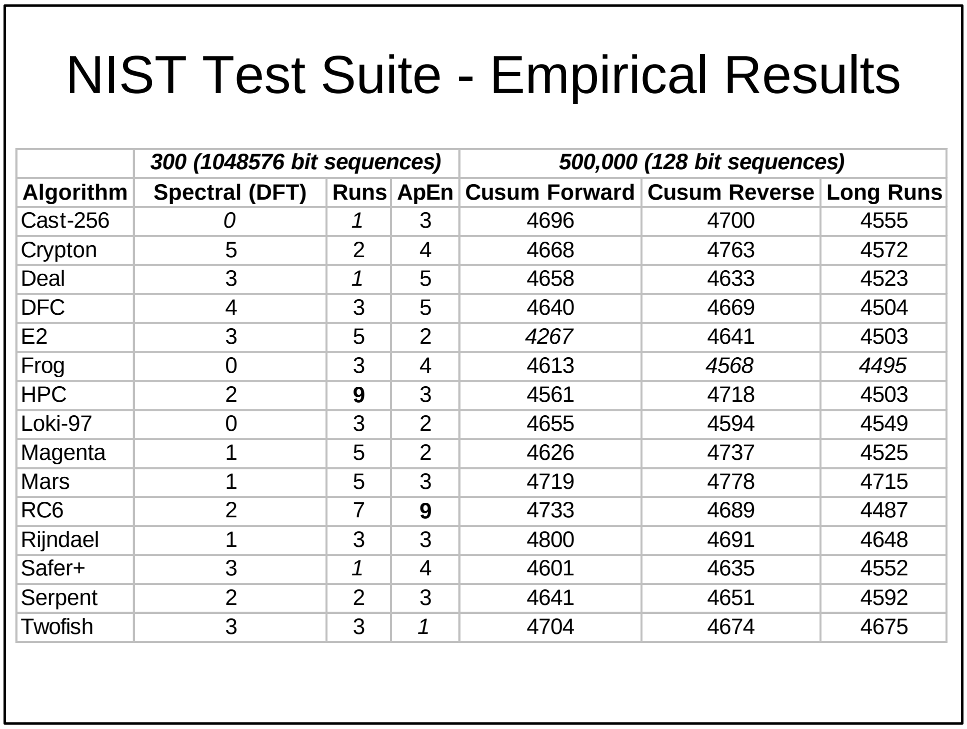
Preliminary Statistical Analysis

- NIST Statistical Tests
  - Spectral (DFT), Runs, Approximate Entropy
  - Cusum Forward, Cusum Reverse, Long Runs
- Crypt-XB Statistical Tests
  - Frequency, Binary Derivative,
  - Linear Complexity
- DIEHARD Statistical Tests



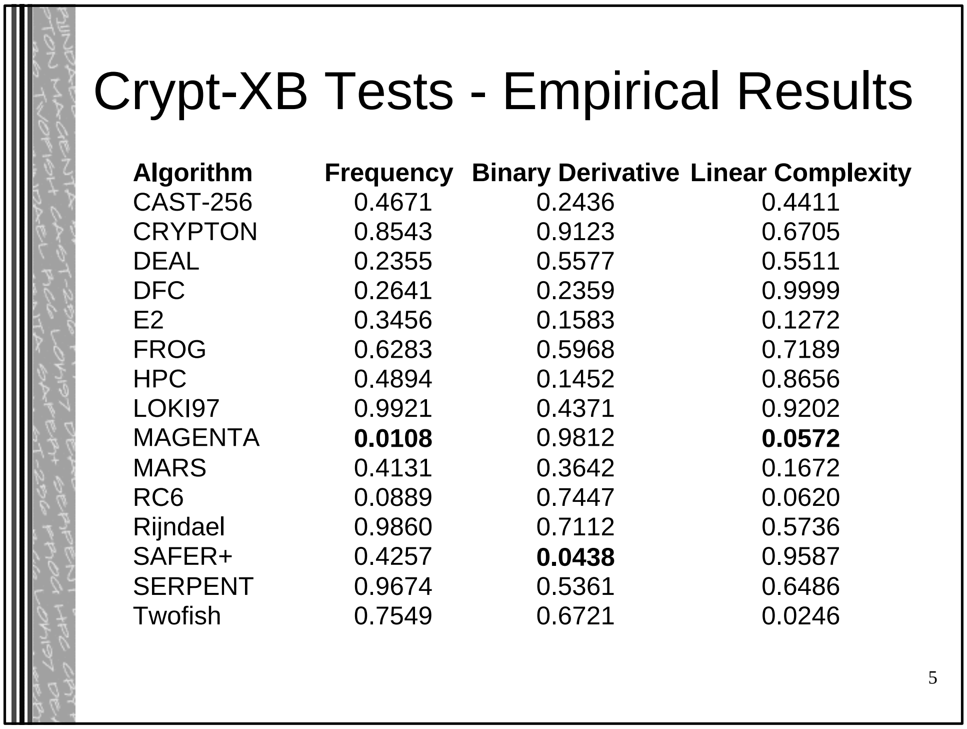
Data Analyzed

- **Cipher Block Chaining (CBC) Mode Data**
  - 39 MB, 300 keys, Null IV & Null Plaintext.
- Special Avalanche Inputs
  - Key [Plaintext]/Ciphertext Avalanche
- Special Plaintext Inputs
  - Low [High] Density Plaintext/Ciphertext
- Special Key Inputs
  - Low [High] Density Key/Ciphertext
- Plaintext/Ciphertext Correlation



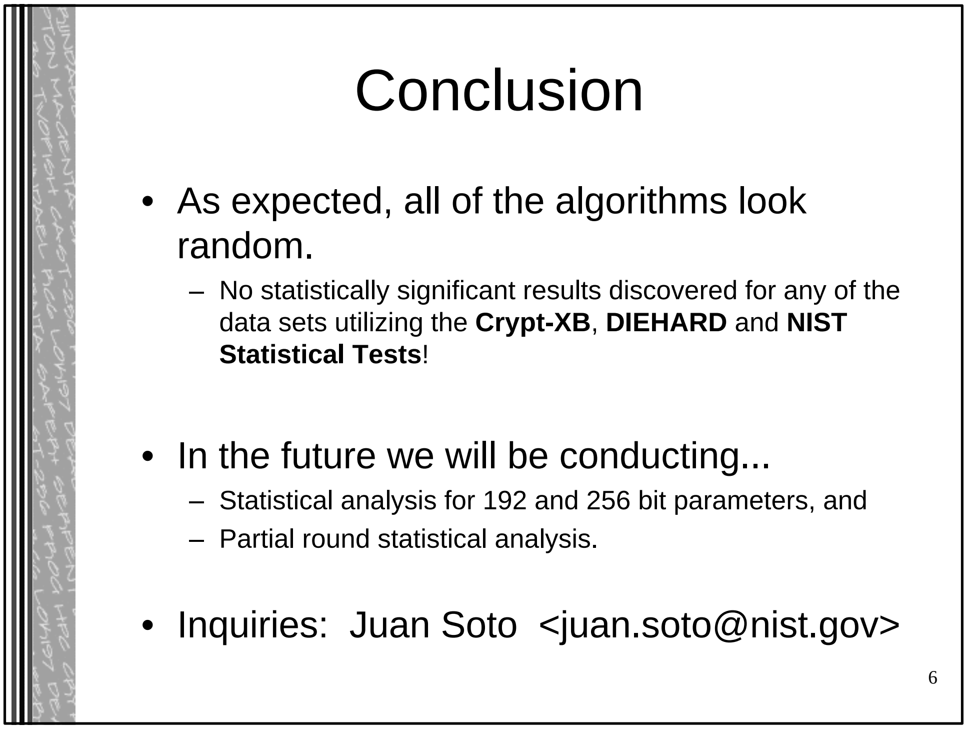
NIST Test Suite - Empirical Results

	300 (1048576 bit sequences)			***500,000 (128 bit sequences)***		
Algorithm	**Spectral (DFT)**	**Runs**	**ApEn**	**Cusum Forward**	**Cusum Reverse**	**Long Runs**
Cast-256	*0*	*1*	3	4696	4700	4555
Crypton	5	2	4	4668	4763	4572
Deal	3	*1*	5	4658	4633	4523
DFC	4	3	5	4640	4669	4504
E2	3	5	2	*4267*	4641	4503
Frog	0	3	4	4613	*4568*	*4495*
HPC	2	**9**	3	4561	4718	4503
Loki-97	0	3	2	4655	4594	4549
Magenta	1	5	2	4626	4737	4525
Mars	1	5	3	4719	4778	4715
RC6	2	7	**9**	4733	4689	4487
Rijndael	1	3	3	4800	4691	4648
Safer+	3	*1*	4	4601	4635	4552
Serpent	2	2	3	4641	4651	4592
Twofish	3	3	*1*	4704	4674	4675



Crypt-XB Tests - Empirical Results

Algorithm	**Frequency**	**Binary Derivative**	**Linear Complexity**
CAST-256	0.4671	0.2436	0.4411
CRYPTON	0.8543	0.9123	0.6705
DEAL	0.2355	0.5577	0.5511
DFC	0.2641	0.2359	0.9999
E2	0.3456	0.1583	0.1272
FROG	0.6283	0.5968	0.7189
HPC	0.4894	0.1452	0.8656
LOKI97	0.9921	0.4371	0.9202
MAGENTA	**0.0108**	0.9812	**0.0572**
MARS	0.4131	0.3642	0.1672
RC6	0.0889	0.7447	0.0620
Rijndael	0.9860	0.7112	0.5736
SAFER+	0.4257	**0.0438**	0.9587
SERPENT	0.9674	0.5361	0.6486
Twofish	0.7549	0.6721	0.0246



Conclusion

- As expected, all of the algorithms look random.
  - No statistically significant results discovered for any of the data sets utilizing the **Crypt-XB**, **DIEHARD** and **NIST Statistical Tests**!
- In the future we will be conducting...
  - Statistical analysis for 192 and 256 bit parameters, and
  - Partial round statistical analysis.
- Inquiries: Juan Soto <juan.soto@nist.gov>