Alternate N-Bit Key Encryption and Secret Sharing Showcase

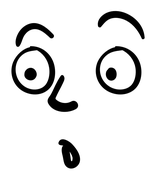
Luna Dagci and Jacob Clouse

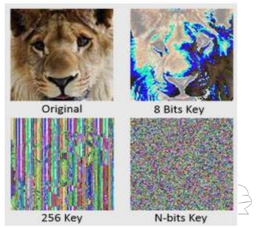
Course: ICSI 526 Cryptography, Professor: Pradeep Atrey

College of Engineering and Applied Sciences, University at Albany, State University of New York

Introduction

- Do we want to protect the confidentiality of our photos?
- Can we reduce the size of the photos in encrypted form?





Alternate N Bit Encryption

Encryption:	
Input:	*MSN == file with nbytes;*
	n == number of blocks of MSN;
	ENCK == encryption key;
Step 1:	*e = HASH(MSN, H0);*
Step 2:	*H1 = HASH(ENCK, H0);*
Step 3:	*BLK[0] = e XOR ENCK;*
Step 4:	*H1 = HASH(e, H1);*
Step 5:	*for (x = 1; x<= n; x++)*
	{
	BLK[x] = blk[x] XOR H1;
	H1 = HASH(H1, H1);
	}
Output:	*BLK[0]...BLK[n];*

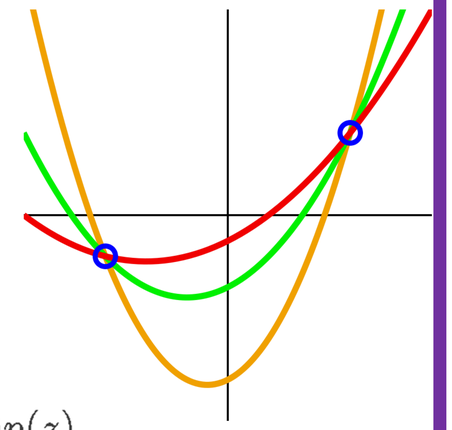
Alternate N Bit Decryption

Decryption:	
Input:	*BLK[0]...BLK[n];*
	ENCK == encryption key;
Step 1:	*H1 = HASH(ENCK, H0);*
Step 2:	*e = BLK[0] XOR ENCK;*
Step 3:	*H1 = HASH(e, H1);*
Step 4:	*for (x = 1; x<= n; x++)*
	{
	blk[x] = BLK[x] XOR H1;
	H1 = HASH(H1, H1);
	}
Output:	*e, blk[1]...blk[n];*
	MSN == blk[1]||blk[2]||...||blk[n];
	//To verify msn integrity:
	e == HASH (msn, H0);

Why this is Important:

Secret Sharing and Homomorphism

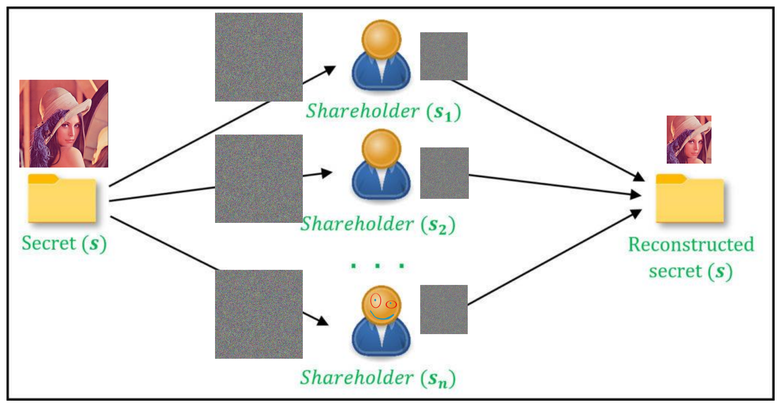
- Shamir's Secret Sharing enables a secret to be split into multiple shares, such that a certain number of shares is required to reconstruct the original secret.



- Polynomial:

$$p(X) = \sum_{z \in Z} L_z(X) p(z)$$

- Lagrange Basis: $L_z(X) = \frac{\prod_{j \in Z \setminus \{z\}} (X - j)}{\prod_{j \in Z \setminus \{z\}} (z - j)}$



References

Alternate N-bit Key Data Encryption for Block Ciphers - Kayque M. C. Damasceno, Carlos A. de Moraes Cruz, Anderson V. C. de Oliveira, Luís S. O. de Castro

Common Cryptographic Architecture (CCA): Cipher Block Chaining (CBC) mode. (n.d.). Common Cryptographic Architecture (CCA): Cipher Block Chaining (CBC) Mode.

M. Mohanty, W. T. Ooi and P. K. Atrey, **"Scale me, crop me, know me not: Supporting scaling and cropping in secret image sharing**," 2013 IEEE International Conference on Multimedia and Expo (ICME), San Jose, CA, USA, 2013, pp. 1-6.

Contact Information: (ldagci, Jclouse)@albany.edu