CSL7480 Cryptography **11 Jan 2023**

Lecture 4: Cryptography

Lecturer: Somitra Sanadhya *Scribe: Nitya Anand Shah (B20CS039)*

Disclaimer: *These notes have not been subjected to the usual scrutiny reserved for formal publications. They may be distributed outside this class only with the permission of the Instructor.*

4.1 In previous class

Perfect Secrecy

Also known as Unconditional security or Information theoretic

Conditions :-
1) Shannon Secrecy -

A cipher (M, K, KeyGen, Enc, Dec) is **Shannon secure w.r.t a distribution** D over M if for all m' ∈ M and for all c,

Pr[m ← D : m = m'] = Pr[k ← KeyGen, m ← D : m = m' | Enc(m, k) = c]

It is **Shannon secure** if it is Shannon secure w.r.t **all distributions** D over M.
Intuitively, this means that:

C contains no NEW information about m

2) Perfect Security -

Scheme (M, K, KeyGen, Enc, Dec) is **perfectly secure** for every pair of messages m1 m2 in M for all c,

Pr[k ← KeyGen : Enc(m1,k) = c] = Pr[k ← KeyGen : Enc(m2, k) = c]

Intuitively, this means that:

Ciphertexts are independent of the plaintext(s)

4.2 OTP : One Time Pad

4.2.1 Mathematical Interpretation

Let n be an integer = length of the plaintext messages.
Message space M := $\{0,1\}^n$ (bit strings of length n)
Key space K := $\{0,1\}^n$ (keys too are length n bit-strings)
The algorithms are:

- **KeyGen**: samples a key uniformly at random k ← $\{0,1\}^n$
- **Enc(m,k)**: XOR bit-by-bit,
  Let m = $m_1m_2...m_n$ and k = $k_1k_2...k_n$;
  Output c = $c_1c_2....c_n$ where $c_i = m_i \oplus k_i$ for every i ∈ [n]
- **Dec(c,k)**: XOR bit-by-bit.
  Return m where $m_i = c_i \oplus k_i$ for every i.

4.2.2 Proof For Perfect secrecy

Let a $\oplus$ b for n-bit strings a, b mean bit-wise XOR.
Then: Enc(m,k) = m $\oplus$ k and Dec(c, k) = c $\oplus$ k.
Ciphertext space is C := $\{0,1\}^n$.
Correctness: Straightforward.
Perfect secrecy: fix any m $\in \{0,1\}^n$ and c $\in \{0,1\}^n$

$$Pr_k[Enc_k(\mathrm{m}) = \mathrm{c}] = \mathrm{Pr}[\mathrm{m} \oplus \mathrm{k} = \mathrm{c}]$$
$$= \mathrm{Pr}[\mathrm{k} = \mathrm{m} \oplus \mathrm{c}] = 2^{-n}$$
$$Pr_k[Enc_k(\mathrm{m}) = \mathrm{c}] = 0\ (\forall\ \mathrm{c} \notin \{0,1\}^n)$$

=> $\forall$ (m1, m2) $\in \{0,1\}^n xn$ and $\forall$ c :
$Pr_k[Enc_k(m_1) = \mathrm{c}] = Pr_k[Enc_k(m_2) = \mathrm{c}]$. (QED)

4.2.3 Remarks

1) Improvement to the Vernam cipher.
2) The Caesar Cipher (Shift Cipher with k = 1) is just OTP for 1-alphabet messages.
3) Mathematically:
   - XOR is the same as addition modulo 2: a+b mod 2
   - Caesar Cipher for 1-alphabet is addition modulo 26
4) The key must be:
   - a random key that is as long as the message.
   - need not be repeated
   - sampled uniformly every time
5) In addition, the key is used to encrypt and decrypt a single message and then is discarded. Each new message requires a new key of the same length as the new message.
6) It produces random output.
7) No statistical relationship to the plaintext.
8) Because the ciphertext contains no information whatsoever about the plaintext, there is simply no way to break the code.
9) The security of a one-time pad is entirely due to the randomness of the key.
OTP yields the ultimate in security.
10) One Time Pad is a perfectly secure private-key encryption scheme.

4.2.4 Fundamental Difficulties

1) The practical problem of making large quantities of random keys.
2) Even more daunting is the problem of key distribution and protection (since it is symmetric)
3) Malleability -
   a) Malleability is often an undesirable property in a general-purpose cryptosystem since it allows an attacker to modify the contents of a message. An encryption algorithm is ”malleable” if it is possible to transform a ciphertext into another ciphertext which decrypts to a related plaintext.
   b) That is, given an encryption of a plaintext m, it is possible to generate another ciphertext which decrypts to f(m), for a known function f, without necessarily knowing or learning m.
   c) For example, suppose that a bank uses a stream cipher to hide its financial information, and a user sends an encrypted message containing, say, ”TRANSFER 0000100.00 TO ACCOUNT .”
   If an attacker can modify the message on the wire and guess the format of the unencrypted

message, the attacker could change the amount of the transaction, or the recipient of the funds, e.g. "TRANSFER 0100000.00 TO ACCOUNT ".

3.1) Malleability does not refer to the attacker's ability to read the encrypted message. The attacker cannot read the encrypted message before and after tampering.
3.2) A cryptosystem may be semantically secure against chosen plaintext attacks or even non-adaptive chosen ciphertext attacks (CCA1) while still being malleable. However, security against adaptive chosen ciphertext attacks (CCA2) is equivalent to non-malleability.

Because of these difficulties, the one-time pad is of limited utility and is useful primarily for low bandwidth channels requiring very high security.

4.3 Shannon's Theorem

For every perfectly secure cipher (Enc, Dec) with message space M and key space K, it holds that $|K| \geq |M|$.
Note: Proof of the same is provided in 3.4.5 in the lecture scribe 3 by Sumit Kumar Prajapati.
- If we could reuse OTP, we could encrypt longer messages with shorter keys.
- Simply break the message into shorter parts.
- Therefore, by Shannon's Theorem, the resulting scheme will not be perfectly secure.
- Even worse — it will be open to the frequency attack! (just like Vigenere Cipher)
- In fact, lots of neat examples where reusing OTP leaks clear pattern. Shannon's Theorem on key length is pretty bad news for perfect ciphers.
- It means we really have to give up on perfect secrecy for practical applications unless we absolutely need it.

The dawn of modern cryptography: we want to construct something that is "just as good for practical purposes." The modern approach focuses on what computers can do efficiently.

4.4 Computational Security

Conditionally or computationally secure cryptography uses a shared secret key of limited length to provide security against an opponent with limited computational resources by making it computationally infeasible to extract the key or message.

Pr[M = m — C = C] - Pr[M = m] $\neq$ 0

$|Pr[M = m|C = C] - Pr[M = m]| \leq$ E(n) ∀ m,C; n = Security Parameter

Earlier the attackers were allowed exponential computations but now they are computationally limited and can perform only poly(n) computations.

Negligible functions (ϵ(n)) :- ϵ(.) : N → R is a negligible function if ϵ(n) $< 1/n^c$ for any c and ∀ n $\geq n_0$
some examples of negligible functions are: 2^{-n}, $2^{-n/2}$

This ensures that even if the attacker is allowed to repeat their activities the probability of their success will still remain negligible.