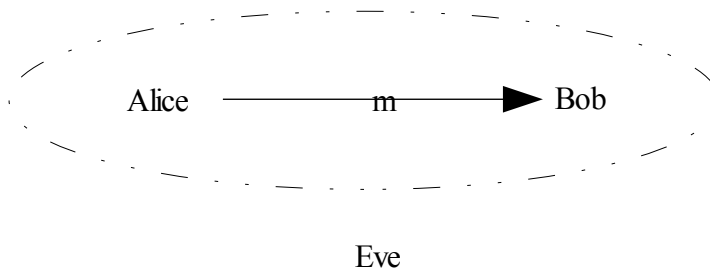


Definition of Security for Encryption:

Ideal World:



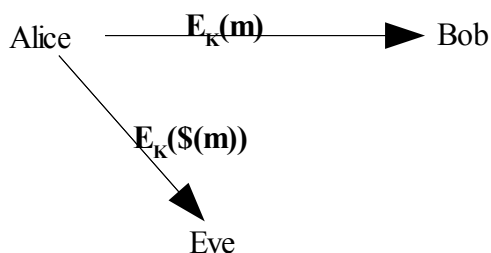
The ideal world for communication should be such that Alice sends a message to Bob and Eve Learns nothing. But in reality this is not possible. Eve can almost always learn that a message was sent and most of the times its length.

We modify our definition of Ideal World accordingly so that we can define security of encryption schemes in a more realistic fashion.

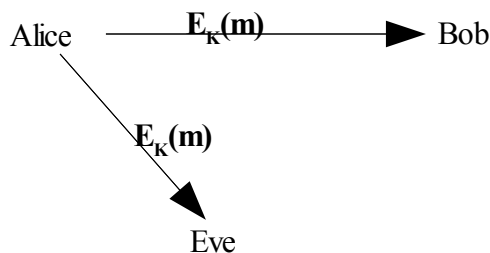
Notation:

$\$(x)$: A random string of the same length as x . $\$$ is non-deterministic hence the same input x will give two different outputs for two different runs.

Ideal World:



Real World:



The only difference between the Ideal World and the Real World is that in the real world, Eve gets the encryption of the message while in the Ideal World she gets the encryption of a random, non-deterministic string of length equal to that of m . Our model of security is that Eve cannot tell which world she is in. This security is called real or random (**R-o-R**) security.

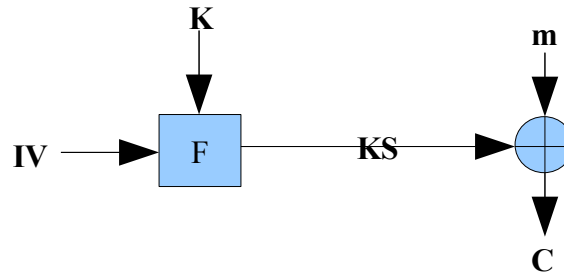
Remark: Here we use encryption of $\$(m)$ instead of $\$(m)$ directly because we do not want to derive the security from obscurity of the encryption scheme. Security from obscurity is particularly bad because once the algorithm is known to the adversary, everything is broken. Also finding out another good algorithm is hard and time consuming. We rather derive the security from the encryption key as it is easy to change if one is compromised and there are many options.

Def:

An encryption scheme is (t, q, ϵ) Real-or-Random(**R-o-R**) secure if for all adversaries A running in time $\leq t$ and making at most q oracle queries (q bits worth of queries):

$$\text{Adv } A = | \Pr [A^{EK} = 1 \mid K \leftarrow U_{\text{keys}}] - \Pr [A^{EKo\$} = 1 \mid K \leftarrow U_{\text{keys}}] | \leq \epsilon$$

WEP Improved:



How to Choose IV:

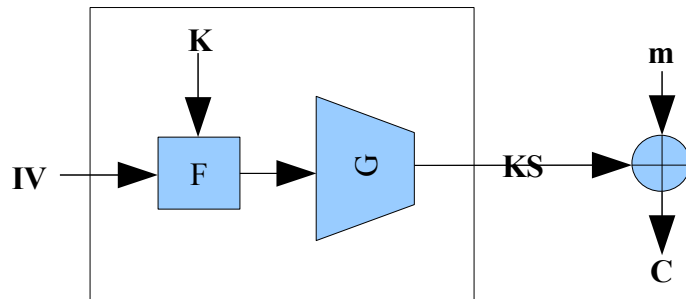
1. Randomly
2. As a Counter
3. ~~As a function of m~~ (bad idea because IV goes in plain with the message and may give the adversary some knowledge about the message)

Problem:

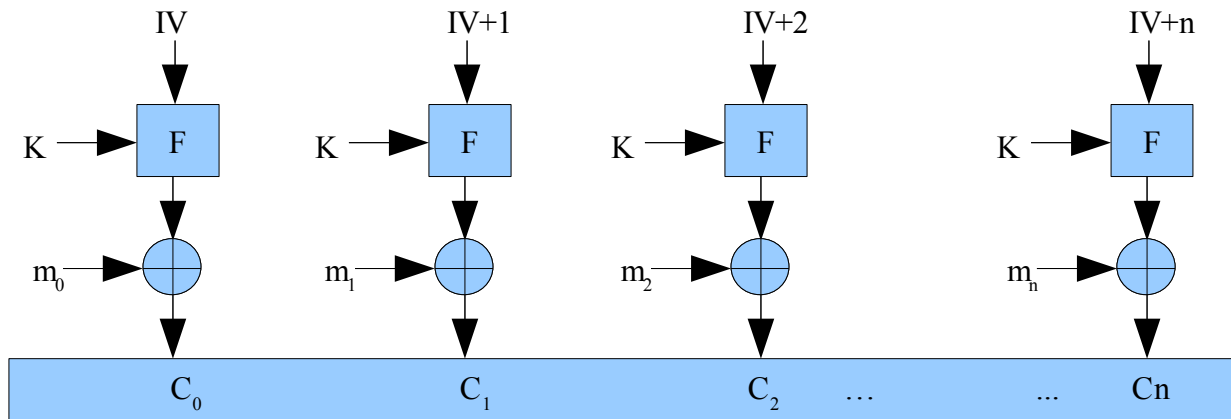
A PRF is $F: \{0,1\}^{128} \times \{0,1\}^{128} \rightarrow \{0,1\}^{128}$ function. How do we encrypt messages longer than 128 bits.

Solution:

1. Use GGM:
Theorem: PRGoPRF = PRF



2. Use Counter Mode:



Counter mode is different from block cipher in that it uses a PRF while block ciphers use PRP. A PRF can map 2 different input values to the same value in the domain but PRP cannot. This is the reason why PRP is invertible but PRF is not.

The two modes for choosing the IV are:

1. **CTR^F\$**: Pick a random IV for each message.
 - No state information required. Easy to implement.
 - Frequent IV collisions due to birthday paradox
2. **CTR^F**: Pick one IV at the time of system boot-up and keep incrementing it.
 - IV collision only after exhausting all values
 - May not have to send IV each time
 - Synchronization is required if system crashes. State to be maintained.

Theorem: If F is a (t, q, ϵ) secure PRF then **CTR^F** is $(t - O(q), \min(q, |\text{ctrs}|), \epsilon)$ **R-o-R** Secure. (Here q is total number of message blocks as one query (m) to the system may actually be many queries to the system.)

Fact: $U_1 \text{ XOR } D_1 = U_1$

Prove: $E_{k0\$} = \text{CTR}^{\text{FK}}$

By DPI-PRF $\text{CTR}^{\text{FK}} \sim \text{CTR}^{\text{R}} \dots\dots\dots(\text{I})$

Using the fact specified above, **CTR^R** generates a uniform distribution by combining a random stream (the output of random function R) to the input.

Also **E_{k0}\$** generates a uniform distribution by combining a random stream ($E(\$m)$) with the output of F .

As both the constructions generate uniform distributions, they are equivalent:

$\text{CTR}^{\text{R}} \sim E_{k0\$} \dots\dots\dots(\text{II})$

Combining I and II, we get

$E_{k0\$} = \text{CTR}^{\text{FK}}$

Hence we have proved that if IV does not repeat, **CTR^F** (counter mode choosing IV in a series), is a real-or-random secure encryption scheme.

Theorem: If F is a (t, q, ϵ) secure PRF then **CTR^F\$** is $(t - O(q), q, \epsilon + (q^2/2|\text{ctrs}|))$ **R-o-R** Secure. (Here q is limited by birthday paradox. This scheme has a worse security but is stateless and hence easier to implement and manage as compared to the previous one)