One-time Pad

$X \in \{0,1\}^n$
$K \in_R \{0,1\}^n$
$E(X,K) := X \oplus K$
$D(Y,K) := Y \oplus K$

Usefulness of OTP:
- never repeat keys!
- codebook
- replace randomness by pseudorandomness
- attacker toggles $Y[i] \to$ toggles $X[i]$

Generalize

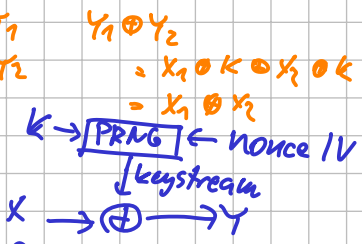
G group $(G, +, 0, -)$
$X, Y, K \in G$ $K \in_R G$
$E(X,K) = X + K$
$D(Y,K) = Y - K = Y + (-K)$
$\forall X \forall Y \exists! K : X + K = Y$ $(K = Y - X)$
$\Pr[\_] = \frac{1}{|G|}$

$\mathbb{Z}_t = \{0, \dots, t-1\}$ mod t
Zog

Def: A cipher is perfectly secure $\equiv$
$\forall X \forall Y \Pr_K[E(X,K) = Y]$ is constant
$[D(Y,K) = X]$

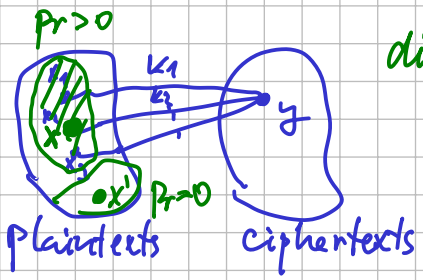
OTP is perfectly secure.

$X_1 \oplus K = Y_1$
$X_2 \oplus K = Y_2$
$Y_1 \oplus Y_2 = X_1 \oplus K \oplus X_2 \oplus K = X_1 \oplus X_2$



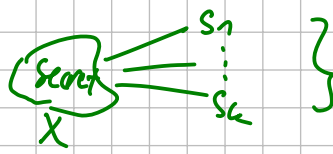
Thm: If #keys < #messages, then the cipher is not perfectly secure.

Proof:



distribution on plaintexts isn't uniform

Information-theoretic Security (Shannon security)



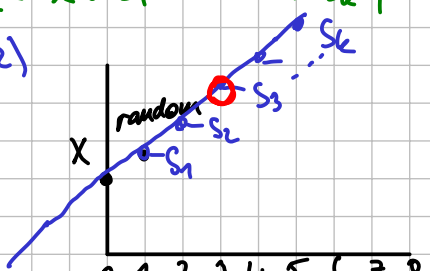
Secret sharing (splitting)

(1) S_1 = random $S_1 \oplus S_2 \to X$ (2,2)
$S_2 = X \oplus S_1$

(2) $S_1 \dots S_{k-1}$ = random
$S_k = X \oplus S_1 \oplus \dots \oplus S_{k-1}$

$\bigoplus_i S_i = X$
(k,k)

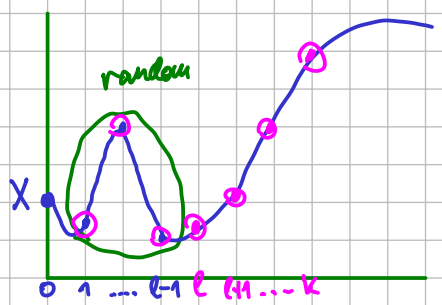
(3) $(k,2)$



Def: (k,ℓ)-threshold scheme
Split X to shares $S_1 \dots S_k$
s.t. any ℓ shares give X
with $< \ell$ shares: no information on X

work in finite field F
looking for $f(x) = ax + b$
$f(0) = X$
$f(1) \in_R F$
$S_1 \dots S_k$ $S_i := f(i)$

(4) (k,ℓ)



Polynomials of degree $< \ell$
unique poly p
Shares: $S_i := p(i)$

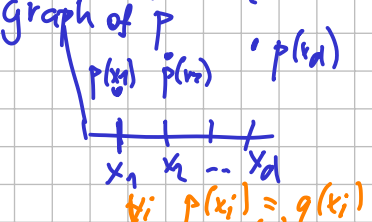
Polynomials over F

(A) If $x_1 \dots x_t$ are all the roots of p, then $p(x) = (x-x_1)(x-x_2) \dots (x-x_t) \cdot q(x)$ (no roots)
$\Rightarrow$ A non-zero p of deg d has at most d roots

(B) Let p, q polys of deg $< d$ with the same graph, then $p = q$.

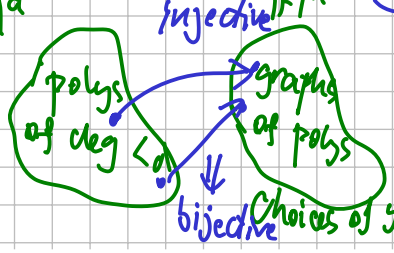
Proof: $r := p - q$ deg $< d$
$x_1 \dots x_d$ are roots of r
$\Rightarrow r = 0 \Rightarrow p = q$.

$x_1 \dots x_d$ distinct
graph of p: $p(x_1)$ $p(x_2)$ $\dots$ $p(x_d)$



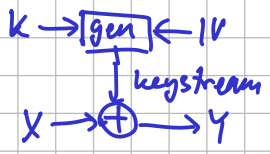
$\forall i \; p(x_i) = q(x_i)$
$r(x_i) = 0$

injective $|F|^d$



(C) For every $x_1 \dots x_d$ distinct and $y_1 \dots y_d$
$\exists!$ p poly of deg $< d$
s.t. $\forall i \; p(x_i) = y_i$
Lagrange Theorem

Symmetric Ciphers



$D_k = E_k$

$X \oplus k_1 \oplus k_2$

$E_k(\overline{x}) = \overline{E_k(x)}$

$E_{k_1}(E_{k_2}(x)) = E_{k_2}(E_{k_1}(x))$

- block ciphers
- stream

block ciphers

work on fixed-size blocks of b bits

Later: use on multi-block messages

$E: \{0,1\}^b \times \{0,1\}^k \to \{0,1\}^b$

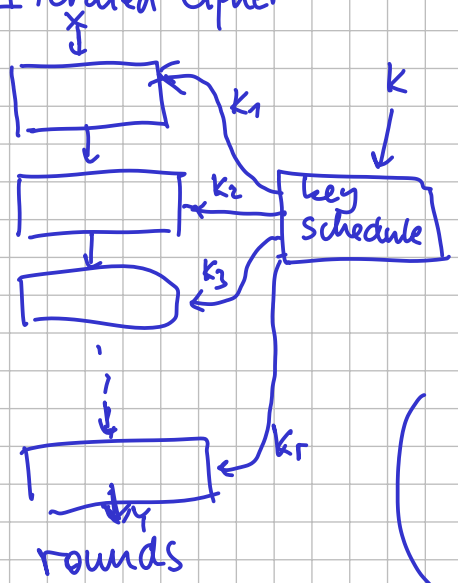
$E_k: \{0,1\}^b \to \{0,1\}^b$ bijection (permutation on set of block values)

In real constructions: almost always even permutation

Security of block cipher

Secure $\Leftrightarrow$ $\nexists$ a distinguisher with $Pr[\text{success}] \geq 2/3$ and run time $< 2^{\text{security level}}$

Iterated Cipher



rounds

Substitution-Permutation Network

Round:

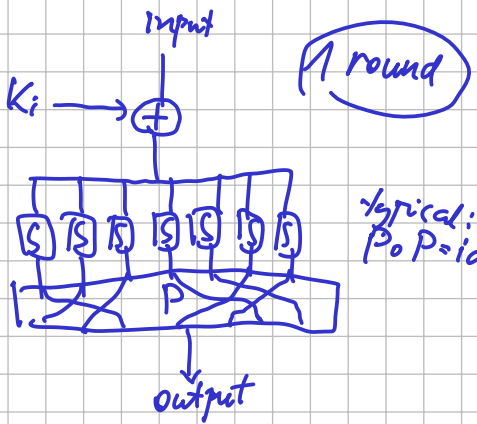
- S-boxes  bijective
  confusion
- P-box permutation on positions
  diffusion
- mixing K_i by $\oplus$

Round is invertible

Inverse of SPN is again SPN

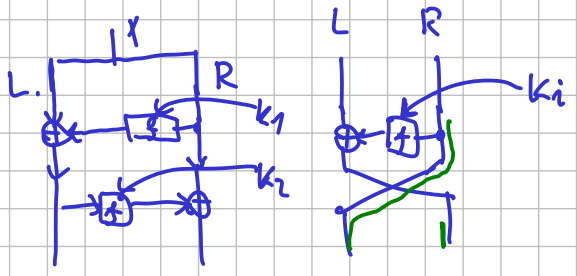
inverse P

inverse S



typical: $P \circ P = id$

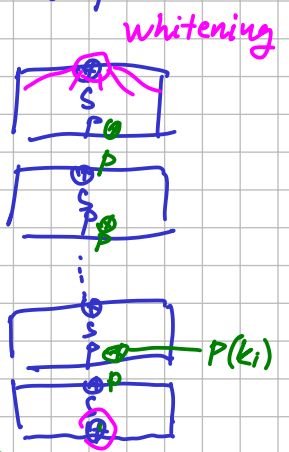
Feistel Network



1 round of FN

inverse of FN is again FN

a Feistel network



DES (Data Encryption Standard)

- developed in 1970's by IBM contracted by NBS influenced by NSA
- 64-bit blocks & 56-bit keys
- S boxes were replaced by NSA at the very last moment

- all 8 S-boxes are different

Expansion:

P is not an involution.

Feistel function: